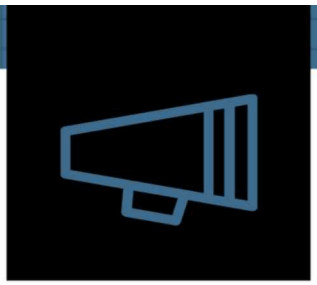
CRYPTOCURRENCY ETHEREUM

HICHAM AND MOHAMED IBNALKADI

VISIT…



ETHEREUM

ASPECTS & TECHNICALITIES

Table of Contents

CHAPTER 1 - Blockchain and Cryptocurrency
Blockchain: Three Parts
- Peer-to-peer networking:
- Asymmetric cryptography
- Cryptographic hashing

Blockchain technology in different spheres
- Digital Identity
- Distributed Cloud Storage
- Smart Contracts
- Digital Voting

Cryptoeconomics and Security
Introduction to Cryptocurrency
First Cryptocurrencies
Pros and Cons of Cryptocurrencies
- Pros:
  - Transparency
  - The Chances of Inflation are highly unlikely
  - Users control their money
  - Transactions cannot be traced
  - Security
- Cons
  - Trust
  - Unrecoverable
  - Untraceable
  - Unstable
  - Limitations
  - Regulation

Gresham's Law
Better Money: A Future Path
Chapter 2 - Ethereum
Ethereum vs. Ethereum Classic
Ethereum Chains and Movement
Ether: Currency and Commodity
Blockout History
Chaos in the Crypto World
Protocol's Power

Trustless System: A Build
Commerce: An Addition
Content Creation
Source Data
Mining 101
Ether and Electricity Prices
Browser vs. Wallet or Keychain
Advantages of Ethereum
- “No downtime, censorship, or third-party interference.”
- “A secure, free, and open platform for the Internet of Things”
- “Enabling transparent governance for communities and businesses.”
- “Handles user authentication and secure payments for you, as well as messaging and even decentralized storage”
- “No need to sign up and pay for application host; the world’s first zero-infrastructure platform”
- State of Smart Contract Development Today

Copycat Coins
Project Funding
Newbie Programmers: A Heads Up
Ethereum: Free and Open Source
Private and Public Chains
Send and Receive Ether
Write Smart Contracts
Create Provable Fair Applications
Launch Your Token
The Promise of Decentralized Databases
What’s Next: New Ways of Working
CHAPTER 3 - The Mist Browser
Wallets as a Computing Metaphor
Ether Address
Where Is My Ether?
The Bank Teller Metaphor
Assets in Cryptocurrency
Visualizing Ethereum Transactions
Breaking with Banking History
Trust to Encryption
- Asymmetric cryptography
- Public-key cryptography

- Symmetric Encryption
- Asymmetric encryption
- Secure Messaging
- Secure and Signed Messaging:
- Digital signature

Mist Installation: System Requirements
Tools for Developers
Working with Messages and Transactions
Transactions Change State
Editing a Global Database
Blockchain: A Revelation
Paying for Transactions
Understanding Denominations
Getting Ether
Anonymity in Cryptocurrency
CHAPTER 4 - Ethereum Virtual Machine
The Central Bank Network of Yesterday
Virtual Machines 101
The Role of the Ethereum Protocol in Banking
Anyone Can Make a Banking Platform
What the EVM Does
EVM Applications Are Called Smart Contracts
Smart Contracts
The EVM Runs Bytecode
Understanding State Machines
Digital vs. Analog
Statements
Data's Role in State
How the Guts of the EVM Work
The EVM Constantly Checks for Transactions
Creating a Common Machine Narrative of What Happened
Cryptographic Hashing: Hash Functions
Blocks: The History of State Changes
Understanding Block Time
The Drawbacks of Short Blocks
"Solo Node" Blockchain
Distributed Security
Mining's Place in the State Transition Function

Renting Time on the EVM
Gas 101
Gas: Importance
Fees as Regulation
Gas Specifications
How Gas Relates to Scaling the System
Accounts, Transactions, and Messages
  Externally Owned Accounts
  Contract Accounts
  Transactions and Messages
  Characteristics of Transactions
  Characteristics of Messages
CHAPTER 5 - Smart Contracts and Tokens
EVM as Back End
Smart Contracts to Dapps
Assets Backed by Anything
Bartering with Fiat Currency
Ether as Glass Beads
Cryptocurrency Is a Measure of Time
Asset Ownership and Civilization
Your Pile of Savings = Reputation
Money, Tokens, and Reputation
Coins are Collectibles
The Function of Collectibles in Human Systems
Early Counterfeiting
Jewelry and Art as Money
The Step toward Banknotes
Platforms for High-Value Digital Collectibles
Tokens Area Category of Smart Contract
Tokens as Social Contracts
Tokens are a Great First App
CHAPTER 6 - Mining Ether
Ether’s Source
Mining: A Definition
Versions of the Truth
Difficulty, Self-Regulation, and the Race for Profit
  Difficulty
Factors Required for Block Validation

How Proof of Work Aids in Block Time Management
What's going on with the DAG and Nonce?
All This for Faster Blocks?
Making Fast Blocks Work
References

CHAPTER 1
Blockchain and Cryptocurrency

A blockchain is a decentralized, peer-to-peer software network that uses encryption to securely host programs, store data, and digital transfer assets equivalent to real-world money. The art of communicating using coded signals is known as cryptography. It is employed in Bitcoin and Ethereum to create a safe computing environment out of thousands of comparable devices, with no central authority and no single owner. With such promise, it's no surprise that the technology has sparked unparalleled conjecture, enthusiasm, uncertainty, and prognostication.

The phrase "Ethereum" can refer to three things:

- **Ethereum Protocol**
- **Ethereum Network** (built by computers that follow the protocol)
- **Ethereum Project** (funds the Ethereum Protocol and Ethereum Network)

Ethereum has developed into a microcosm of its own, attracting enthusiasts and engineers from a wide range of professions. Many of civilization's most annoying flaws could be addressed by blockchains killer apps, with the Ethereum protocol primarily regarded as the network on which these "distributed" apps will emerge. There's no better time for developers, designers, and product managers to start prototyping Ethereum apps.

Non-programmers with interest in Ethereum's possibilities, such as

those who work or have an interest in financial services, consultancy, insurance, legal, game development, government, logistics, product design, or information technology, are two large groups of thinkers interested in blockchain systems, and Ethereum in particular. This gives programmers and non-programmers alike a context to create ideas about what to construct and how to do it. It bridges the gap between computer science, economics, financial services, and banking history, as needed. The difficult part about Ethereum for programmers isn't usually the code; like most open-source software projects, it has on-ramps for people who have already programmed in other contexts. Instead, the difficulty in grasping the concept of "crypto-economics," or the system of incentives and disincentives that ensures the network's security. The issue for non-programmers is predicting how the ecosystem will evolve and how you will fit it. Claims that blockchains will modernize banking, revolutionize insurance, and eradicate counterfeiting may be exaggerated, but to what extent?

Blockchain technology allows for value exchange to take place without the presence of trust or a predominant authority. This technology is thought to be considered one of the best inventions ever created. Picture the scenario below:

Jerome and his best friend bet $100 on a Boxing match between Manny Pacquiao and Floyd Mayweather at MGM Grand Arena over the weekend. Jerome will bet that Manny Pacquiao will win, and your best friend will bet that they will lose or draw.

There are three options to handle this transaction:

1. Both can put their trust in each other regarding the bet. Win or lose, and

the losing party will give the $100 to the winning party. If they are companions, this would be a good way of handling the bet. However, when it comes to paying bets, even the closest friends can fail to settle.

2. The bet can be converted into a contract. The presence of a contract will make a chance more official, and it will also make both parties more susceptible to paying. Should one of the two parties decide not to fulfill their obligation, the winner will have to pay additional funds to cover the legal costs of attaining their money – this could take a long time, too. For a small amount of cash, like $100, this does not sound like an advisable way to manage this transaction.
3. Both can incorporate a neutral third party into this transaction. Both parties will give $100 to the third party, and they will provide the total sum to the winner of the bet. This is a risky option, though, because the third party could end up fleeing with the money. This leaves us with the first two options: trusting each other or resorting to a contract.

It is clear from the discussion that trust and contract are not the most excellent solutions. It's difficult to trust strangers and even friends. Also, enforcing a contract takes a long time and a lot of money. Blockchain technology offers an option for more secure, efficient, and affordable than the other options mentioned above.

Blockchain gives a chance to write several lines of code – on a program that is operating on the blockchain – to which both parties will send $100. The program will keep the $200 safe until the boxing match has been played. Once the result is final (Win or Lose/Draw), the program will transfer the entire amount of money to the winning party. Both parties can check the logic behind the contract, and once the program is running, the blockchain cannot be changed, stopped, or interrupted. Now, this option might sound too advanced for a $100 bet, but when it comes to selling a house, a company, or

a more significant asset, this option is the best one to consider.

Blockchain technology permits digital information to be distributed safely, without the risk of it being stolen or duplicated. As time progresses, various forms of Blockchain technology are creating the backbone of a newer kind of Internet. Information on a Blockchain exists as a database, a shared but continually updated database. This database is not stored in a single location, allowing for the kept records to be authentically public and easily verifiable. Furthermore, an individual or single entity can't control this technology. This is because identical blocks of information are stored across the crypto network.

Blockchain technology was designed to last, and it consists of a built-in strength that makes it reliable and impenetrable. Since it stores identical blocks of information across its network, this technology cannot be controlled by a single person or entity, and it cannot fail. The fact that it is impenetrable and near impossible to penetrate means that it cannot crash. As mentioned earlier, this technology was designed to last. The amount of thought and effort put into this technology ensured that no entity would interfere with the technology, no matter how sophisticated or powerful. A network of computers validates all transactions that occur via this technology. There is always a group of users present to ensure that the transaction list via the technology is accounted for. There is no room for anyone to go rogue because the system was built to prevent that. No one is shut out from accessing the technology, either. For as long as there is access to the Internet, everyone can access Blockchain technology and, after a bit of learning, everybody will be able to understand how everything works. Blockchain technology was not created for a sole set of individuals. It was created with the intent of making it available to the world and to ensure that individuals

can take control of their transactions without needing to rely on an unreliable third party.

Blockchain: Three Parts

A blockchain is a distributed information that is replicated across numerous computers. The ability of this network database to reconcile the sequence of transactions, even when a few nodes in the network receive transactions in different orders, is the innovation symbolized by the word blockchain. This is mainly due to network latency caused by physical distance; for example, a transaction initiated by a user purchasing a hot dog in Tokyo will be sent to nodes in Japan first. An adjacent transaction in Brooklyn has gotten “ahead” of the one in Tokyo by the time a node in New York receives transaction information a few milliseconds later. The discrepancies in distributed systems caused by subjective perspective are what makes them difficult to scale. Blockchain systems are robust because they represent a collection of technologies that can be used to solve the problem.

What is often referred to as a blockchain is a combination of three technologies created by Bitcoin’s pseudonymous inventor. The following are the three ingredients:

Peer-to-peer networking: A collection of computers, such as those in the BitTorrent network, may communicate with one another without relying on a single central authority and avoiding creating a single point of failure.

Asymmetric cryptography: A method for these computers to transmit an encrypted message to specific recipients, with anyone verifying the sender’s identity, but only the intended recipients can read the message’s contents. Asymmetric cryptography is used in Bitcoin and Ethereum to

construct a set of credentials for your account, ensuring that only you may transfer your tokens.

Cryptographic hashing: A method for creating a short, unique "fingerprint" for any data, enabling for rapid comparison of big datasets and a secure technique to ensure that data has not been tampered with; The Merkle tree data structure is used in both Bitcoin and Ethereum to store the canonical order of transactions, which is subsequently hashed into a "fingerprint" that acts as a point of comparison for network computers and around which they can swiftly synchronize.

Experiments with digital money in the 1990s and early 2000s resulted in the fusion of these three elements. Adam Back created Hashcash in 2002, and it was the first cryptocurrency to employ mining to send transactions. The pseudonymous Satoshi Nakamoto added marked the invention with the launch of Bitcoin in 2009. These three parts can be used to simulate a rudimentary database that is decentralized and stored in the network's nodes. Bitcoin can be thought of as a machine, similar to how a swarm of ants forms a functional colony.

Ethereum extends the Bitcoin virtual machine's paradigm in computer science words by introducing a trustworthy global object framework messaging system. The first time Ethereum was proposed was in the Ethereum White Paper, which was published in 2014.

Blockchain technology in different spheres

Digital Identity

Digital identities are always at risk of being stolen or corrupted. Data breaches occur at a more rapid rate, and many companies and systems have been left vulnerable. There was a time that an estimated 70 million customers had personal information that included their names, addresses, phone numbers, and email addresses hacked during the data breach. Hackers got access to millions of users' personal information, and there was little the victim could do about it.

Hacked databases and accounts that have been broken into are the major areas of growing problems in a society that is becoming technologically advanced at a rapid rate. With every day that passes, users must give their personal information to sites whether they like it or not. As a result, many internet users have been left uneasy as they worry about the safety of their digital identities.

Protecting Digital Identity has become one of the most expensive tasks for the world. According to a report by Distil Networks, the annual cost of protecting digital identity and fighting fraud is an estimated $18.5 billion. Simply broken down, for every $3 that is spent, $1 is going to fraud. Moreover, the more protection rolled out to keep individuals' digital security secure, the more severe the onslaught from fraudsters becomes.

Blockchain technology has allowed for the tracking and maintaining of digital identities to become far more secure and efficient. This has led to reduced fraud and ease in signing on to platforms. As the world advances in technology, the use of physical records dwindles. For digital security to become impenetrable, Blockchain technology has to be incorporated into

systems around the globe. This technology can be gained and transferred across several platforms – banking, healthcare, online retailing, identity authentication, etc.

Most security systems make use of password-based systems that can be cracked very easily. Blockchain-based verification systems are based on real identity verification that uses digital signatures founded in cryptography – public-key cryptography, to be precise. When it comes to checking Blockchain identity verification, the only check required is to confirm whether the correct private key was signed or not. This key cannot be duplicated. When someone tries to duplicate the key or steal it, their attempts will be refuted by the system.

Distributed Cloud Storage

It has been predicted that Blockchain data storage will take over traditional forms of cloud storage in the next three to five years. The problem with most cloud storage today is that they are centralized. Users of these different platforms (iCloud, Dropbox, etc.) have no choice but to depend on a single storage provider. The cloud storage servers "control" all online assets that are uploaded. In recent times, we have witnessed the hacking of these cloud storage systems and the repercussions it has had in the lives of many high-profile individuals.

When it comes to using Blockchain technology, the cloud storage system becomes decentralized. Take Storj – a beta-tested cloud storage system that makes use of Blockchain technology – for example. This application has improved security and has relieved the level of dependency users have on the system. The Blockchain-powered system prevents users' assets from being accessed by hackers and other malicious entities. It's no wonder that this technology is about to take over the cloud storage sphere.

Smart Contracts

One phrase that will continue to appear in Ethereum is the concept of a smart contract. A smart contract is a piece of business logic that operates on the Ethereum network, semi-autonomously moving value and enforcing payment arrangements between participants.

Smart contracts are frequently compared to software applications. However, this is an oversimplification; they are more akin to the concept of classes in traditional object-oriented programming. When developers talk about “creating smart contracts,” they usually mean developing code in the Solidity programming language to run on the Ethereum network. Units of value can be exchanged as readily as data when the code is run. As previously indicated in this chapter, digital money holds enormous promise. But, exactly, how does it work? In a decentralized system, how can data behave as money?

An object in computing is typically a tiny bit of data—information—encapsulated in a specific structure or format. This data is frequently accompanied by methods that describe how the object can be used or accessed. Let’s pretend the information contained in this object is important to someone, and that person is prepared to pay to have a method that displays it invoked.

Let’s pretend that a user wishes to pay a small charge to use a cake recipe that they found online. In our example, this recipe is the data object. At the most basic level, the attributes of the cake object, together with the methods, are stored at a specific address in any device's memory.

This depicts the characteristics of a cake and includes a method for the computer to show instructions on how to mix these elements to make the cake. By storing the data in this manner, the program and programmer can easily switch out attributes without updating the code for the display instructions. Objects, in other words, are modular bits of data that may be merged and recombined as needed. This is vital to remember when we cover the anatomy of the blocks that make up the blockchain in later chapters.

This is a process on how computers “move” data to benefit their human users. You can write functions in Ethereum that send money around, just like this small object’s mixing instructions method can display the mixing instructions for a cake when called.

In recent years, the usage of paper and physical records has decreased worldwide as businesses and individuals increasingly rely on digital records to retain information, including contractual agreements.

Smart contracts are digitized contracts that are just as legally binding as hardcopy agreements. These contracts are entered on the blockchain and are programmable. Developers implement these contracts as variables – and statements – that can release funds via the bitcoin network. This is considered a far more viable option than entrusting such decisions with single, centralized authorities.

For example, if two persons want to trade funds at a specific period in the future, the payout and details of both parties will be programmed into the smart contract once a set of instructions and prerequisites have been met. Once the requirements have been met, the funds will be released and received by the relevant parties. This makes the business far more efficient and the

legal system more reliable.

Digital Voting

One of the biggest challenges when it comes to online voting and other electoral processes is security. By using Blockchain technology, a voter will be able to successfully transmit their vote – while maintaining their anonymity to the rest of the world. This is a digitalized version of how the physical voting process takes place. A Danish political party became the first political group to deploy Blockchain technology during the voting process in 2014. Observers have noted that digital voting, using Blockchain technology, would eliminate various challenges that the current electoral process experiences – thrown votes, duplicated votes, etc.

Cryptoeconomics and Security

One rationale for bringing up currencies and commodities in the context of smart contracts is to practice thinking in terms of creating economic systems entirely in software. That is Ethereum's promise. The burgeoning topic of crypto-economics, which we will examine alongside the technical lessons in this book, is the construction of software systems with game-theoretic rules. When expressed in code, what appears straightforward at first—an equity coin—becomes a world of intricacy. What makes Ethereum and Bitcoin so secure is that they don't rely on any hack-proof technology to keep bad actors at bay; instead, they rely on enormous financial incentives and disincentives.

These are appealing value propositions that should pique the interest of any engineer and software designer. However, getting people enthused about end-user applications while establishing currency (or scrip) coins is a far different challenge. Although financial services may be the most obvious application of this software, future applications may employ the same levers for entirely different objectives.

Introduction to Cryptocurrency

Cryptocurrency is a digital currency that is recorded in a ledger. This ledger contains information on accounts and transactions that occur between peer users who are using the system. The system that enables the use of cryptocurrency is Blockchain technology. Blockchain is a ledger of all transactions between peer users; this ledger also happens to be decentralized. By using this technology, participants can confirm transactions without the need for a central validating authority – a bank, for example.

Cryptocurrency is known as a medium of (financial) exchange. It is created and stored digitally in the blockchain. Encryption methods are used to manage the financial units' creation and verify every transfer of funds. The cryptocurrency was created in response to the displeasure with the current centralized systems. The goal of its creation was to serve as an improvement to the flawed systems that currently exist. The currency is based on decentralized technology, allowing users to make far more secure payments than a centralized or unreliable third party. Money can be transacted and stored in anonymity. Every transaction is recorded in the ledger – no matter how big or small it may be.

Bitcoin transactions have no costs attached to them. All transactions are grouped into blocks. A new block is created, processed, and added to the blockchain six times an hour. All transactions are recorded in the blockchain ledger. The ledger is kept functioning by users known as "miners" – users with powerful computers that can "crunch" transactions that lead to being rewarded in bitcoins – a form of cryptocurrency.

The cryptocurrency was created by Satoshi Nakamoto – an internet

user who prided in his activities being kept on the low-key. Immensely displeased with the current centralized systems, Nakamoto resorted to creating a transacting monetary unit in a more secure, decentralized system. As a result, he invented bitcoin in 2008 before it went online a year later. There have been many attempts to identify Satoshi, but no investigation has ever yielded sufficient results.

Many individuals cherish money that is free of government control and bank fees. Moreover, the fact that the money is secure in the Blockchain system and transactions are verified and processed in anonymity has drawn many people into the cryptocurrency world.

Another benefit found in cryptocurrency is that transactions cannot be faked or reversed – common errors seen in the bank systems. Transactions are airtight, relieving pressure on many users who make use of the platform. The incredibly low fees for transactions also make cryptocurrency far more trustworthy than traditional currency. The fact that the currency is decentralized means that there is open access to everyone – contrary to the exclusive systems perpetuated by banks. Transactions run on a peer-to-peer network, adding to the open and transparent nature of cryptocurrency. There is no single entity that claims responsibility or control over the system. It is a currency designed for the people, free from third-party restrictions. Once a transaction is permitted, it cannot be altered by anybody. If you send money, it has been sent, and it cannot be recovered. That is why every transaction that takes place needs to be done with ample care and attention.

As mentioned earlier, transactions are not connected to real-life identities. Instead, cryptocurrency is reviewed on "addresses," – which appear as random chains that contain up to thirty characters. Thus, the robust system makes it nearly impossible for one's real-life identity to be located through

the blockchain.

Transactions occur instantly in the network and are usually confirmed within a couple of minutes. Location does not matter when it comes to making transactions via cryptocurrency. This is a notable advantage considering the red tape and complications one has to go through when transferring funds from one location to another. Cryptocurrency offers a payment method that requires no permission from any external entity. Once a party decides to send money to someone situated anywhere in the world, once the transaction goes through, it's done. One doesn't have to go through a mass amount of red tape to access cryptocurrency. A free copy of the software is available to anyone. Cryptocurrency – for example, bitcoin – can be used after it has been deployed. Bitcoin – can be sent and received. There are no gatekeepers to be wary of. Once individuals grasp how the system works, they are left to transact as they please.

Users of cryptocurrency often sing its praises, despite the risks that may surround the system. As of July 2017, it was reported that there were a little over sixteen million bitcoins in circulation. In March 2017, the value of one Bitcoin surpassed $1000 for the first time, surpassing the price of an ounce of gold. The value of cryptocurrency has soared since then, and reports have shown that it will continue to increase in this fashion.

First Cryptocurrencies

The development of cryptocurrency has occurred since the late 1990s, with Wei Dai publishing an account of something referred to as "b-money" – a distributed electronic system based on anonymity. Not long after, developer Nick Szabo created "bit gold."

Bit gold was designed as a decentralized digital currency. In Szabo's scheme, a participant was required to use computation power to solve proof-of-work puzzles (also known as cryptographic puzzles). When these puzzles were solved, they would be sent to a public registry, and the solver would be assigned a public key. Every solved puzzle would be incorporated into the following puzzle, thus creating a growing chain of a new property. This part of the system provided a robust method for the network to verify new coins and add time-stamps to them. If most of the parties present on the web disagreed with accepting new puzzle solutions, the next puzzle would not be solved until a consensus was reached.

The problem with bit gold was in the double-spending situation. This problem often popped up when users would attempt to design transactions with digital currency. Once data was created, it would be easy for it to be copied and pasted. To prevent this from becoming a problem, most cryptocurrencies gave up some control to a central authority. This was to ensure that all account balances would be tracked and accounted for. Szabo saw this as an unacceptable solution. Szabo wanted to mimic the security and reliability of real-life gold. To him, the most important thing was to never depend on a central authority, regardless of how trustworthy they appeared to be. The currency was never implemented, but it was said to set a precedent for the architecture behind Bitcoin.

Cryptocurrencies go further than the recent eight-year-old breakthrough. Admittedly, Bitcoin results from numerous failed attempts at digital cash in the late 80s due to the involvement of trusted third-party systems. These failures, as a result, gave way to varying opinions that have kept several people either for, against, or confused about cryptocurrencies.

Bitcoin offers a secure and decentralized way of exchanging money via the Internet. Bitcoin is different because it is an open ledger in which information is distributed to all peers without a third-party overseer. Rather, this Peer Peer system proves trustworthy and guarantees security because each transaction on the blockchain, represented by cryptographic codes, is required to be solved and verified by the consensus of every member. So the risks of transactions winding up in the wrong account or double-spending are avoided.

Pros and Cons of Cryptocurrencies

Pros:

Transparency

With Bitcoin and other cryptocurrencies, an open ledger, known as a blockchain, is where all transactions are accounted for and monitored. Once a transaction has been processed, confirmed, it cannot be altered. Likewise, transactions cannot be revised or reversed once they have entered the ledger. No one within the network can manipulate a transaction, thus giving cryptocurrency one of its biggest security features. All transaction information is available for any user to see – unlike in a bank system where transaction information is kept confidential. Many malicious entities have taken advantage of the bank systems and have manipulated transactions on many occasions. Cryptocurrency offers technology that has lowered the risk of such occurring.

The Chances of Inflation are highly unlikely

When it comes to traditional currencies, inflation is inevitable. Economies lead to shifts in prices, governments print out more money to meet demands, and many other factors contribute to the inflation of the traditional currency. With Bitcoin and other cryptocurrencies, inflation is not experienced on such a wide scale because of an absolute number of minable Bitcoin (and other cryptocurrencies). Bitcoin, for example, was programmed to have an estimated 21 million Bitcoins ever to be mined. The last Bitcoins are estimated to be mined in 2050, with none being introduced to the market afterward.

Users control their money

The purpose of cryptocurrency is to give users the freedom to control

their transactions without relying on a central authority or a third party. Transactions are conducted independently of the identities of the people or companies who are making them. This bumps up protection from identity theft and allows users to make transactions without any worry. Cryptocurrency offers users an opportunity to create seamless transactions without the hassles of having to go through third-party individuals or entities. Transaction fees are much cheaper than traditional bank systems because the transaction goes directly from one party to the next.

Transactions cannot be traced

This can be considered as a good and bad thing. In the light of good, untraceable transactions mean that users can send and receive money without the fear of being monitored by external authorities. Cases of theft and fraud are lowered because hackers and other malicious entities will not intercept transactions with ease. Applications that assist with "blurring" transactions, also known as mixing services, are available for users to patronize if they want to eradicate the chances of their transactions being observed and breached.

Security

There is definite security with Bitcoin. All users control their transactions, and codes cannot be misused or exploited by people, organizations, or the government because of the intricate cryptography. In addition, private information remains hidden, and personal information is not attached to the transactions, meaning that chances of identity theft are completely narrowed down to zero.

Cons

Trust

Cryptocurrency is not as widely known as it should be. Information on Bitcoin and other digital currencies entered the public sphere very recently, but many people are still uninformed on what cryptocurrency is all about. Some people have also denounced bitcoin based on their poor knowledge and publish this information to the general public to discourage people from becoming interested in the topic. The lack of informed individuals has led to fewer people understanding what cryptocurrency is and how it works. People have developed a mistrust of digital currency without taking time to understand it. Many corporations have refused to accept Bitcoin as a form of payment, which has not helped the cause. People who desire to use Bitcoins as a payment method for their day-to-day transactions are limited. There are still levels of knowledge and understanding that have not yet been reached. Therefore people need to be educated about Bitcoin to use it to its full potential and apply it to their daily lives. Companies interested in Bitcoin also need to educate their staff members, which might be time-consuming or possibly expensive.

Unrecoverable

In the traditional transactional system, if someone's account is hacked or falls victim to fraud, measures can be taken for the money to be recovered. Bitcoin, and other cryptocurrencies, however, cannot be retrieved once they are lost. No mechanism can recover lost Bitcoins. If someone's wallet is hacked and their digital currency is stolen, there is no network authority they can report the matter to. This is why users need to be wary of the people they send transactions to. If you fall victim to fraud, no one will be able to help

you. Care must be taken when saving money in a wallet application. Users have been advised to avoid using web-based wallets to save their digital currency. Storing digital currency on a drive that is disconnected from the Internet is one of the best options one can consider; such drives are encrypted for the sake of security.

Untraceable

The fact that bitcoin transactions cannot be traced has both a positive and negative side, as indicated in the "Pros" section. The negative side is that many criminals have resorted to using cryptocurrency to facilitate their transactions. Criminals can send and receive digital currency freely because their identities are not attached to the made transactions. This is why the use of cryptocurrencies has been considered illegal by numerous governments.

Unstable

When trading cryptocurrency like a commodity, users should know that all cryptocurrencies are subject to dramatic fluctuations. The value of Bitcoin could soar today and dive tomorrow. Trading and mining cryptocurrency is not an activity people should consider if all they are sent on is making money. The market is volatile and can lead to causing a lot of anxiety – especially in inexperienced traders and miners. The predictions of cryptocurrency are always changing. The best thing is to embrace the present and make the most of it. One needs to be very wary when investing in cryptocurrency, especially altcoins that have newly emerged. Some currencies show promise in their early stages and end up crashing days, weeks, or months later. Cryptocurrency isn't something one just jumps in. Interested traders need to do their research to be fully aware of what they are dealing with. Cryptocurrency comes with great advantages, but it has its risks too, and they need to be noted.

Limitations

The amount of understanding and teachings available on the web of Ethereum is still meager and insufficient for the upbringing of any new developments. The information present on the Internet is either out of date or just too basic to move further into the deeper knowledge of the developer of Ethereum.

Ethereum is also really complicated to handle. And, due to the broad spectra that is the Ethereum platform, which is designed to withstand and accommodate all kinds of programs for many people, despite its flexibility, there is a limit to making it better for any of the programs being constructed. This is why it might not be as effective as Bitcoin.

Ethereum is still quite unstable. If the Ethereum system crashes because of failed updates, all the developer's work stands at risk of being dragged along too. In addition, every saved project or code will be stored in the blockchain, which is very risky for the people creating complex programs.

People are still trying to understand this new currency; therefore, progress will be slow, but people won't rely on preconceptions with time. They will instead move forward with the accurate mentality.

Regulation

There are no standards or norms regarding the use of cryptocurrencies when it comes to international trade. Regulation is something that needs to be discussed. Some countries have gone to the lengths of deeming cryptocurrency illegal, but this is not feasible. Cryptocurrency holds the

potential to benefit the world in a major way. This idea cannot be thrown out because of the bad seeds that have decided to use cryptocurrency for illegal dealings. International entities – countries, institutions, etc.-must find a way to incorporate the benefits of cryptocurrency for the public. Whether people like it or not, a time will come when the banking system flaws and traditional payment methods will be too blatant to excuse. In today's environment, credit card fraud is a huge problem. Hackers target bank accounts regularly. More people are subjected to identity theft and fraud daily. Cryptocurrency offers solutions to the problems that many people are experiencing.

Gresham's Law

What difference does it make if financial products, contracts, and insurance policies are denominated in a cryptocurrency? What does this mean in terms of Ethereum?

A currency that can be used to purchase many valuable securities and assets is worth conserving. Anyone can design a trustworthy, self-executing financial contract (smart contract) that will move ether in the future using the Ethereum network. This might theoretically allow for long-term financial contracts, giving contract participants a motivation to maintain and use ether as a store of value. Gresham's Law argues that "poor" money drives out "good" money in an economy. It was first applied to gold and silver currency. To put it another way, people save and hoard currencies they expect to grow in value while spending currencies they expect to decline.

Even though the legislation is named after a 16th-century English financier, the principle appears to date back to Medieval works, and indeed to ancient texts such as Aristophanes' poem "The Frogs," which is commonly dated to around 405 BC:

Coins with no alloys, gold or silver that are expertly produced tested, and ring true. Despite this, we never use them! Others pass from one hand to the next...

People have been saving the worth of their labor for millennia in a monetary instrument that will remain constant, appreciate, or inflate in price —rather than something that will fall in value. Cryptocurrencies are very volatile in price, and only a few governments and corporations throughout the

world accept them as of this writing. Decentralized smart contracts are rarely, if ever, used in enterprises today. On the other hand, Fiat currencies created by central banks have a dreadful track record, demonstrating a proclivity for bubbles, depressions, and manipulation. Is cryptocurrency ever going to be actual money, and if so, would it be better than the money we’re used to?

Better Money: A Future Path

People, governments, and corporations use Bitcoin (abbreviated as BTC) to transfer value and purchase goods and services today. They pay a tiny fee to the network each time they send bitcoins, denominated in bitcoins. Ether, which has the ticker sign ETH, can be utilized in the same way. For starters, ether can be used to pay for the execution of programs on Ethereum's network. These programs can move at any time in the past, present, or future, as long as specific parameters are met.

Ether can also be regarded as a commodity, similar to fuel for the network to run applications and services, because of its ability to pay for the execution of transactions in the future. As a result, it differs from bitcoins in terms of inherent worth; it is more than just a store of value.

Because fiat currencies are so widely used now, cryptocurrencies may be worse money—that is, more prone to becoming worthless in the long run. Despite this, bitcoin and ether are well-known for being hoarded by their owners, with at least one corporation, Grayscale, a subsidiary of Digital Currency Group, holding them in trust as of this writing.

With the bitcoin incentive halving every four years, global monetary policy issues, general economic instability, and diminishing faith in fiat currencies, higher prices are luring massive amounts of latent "hoarded" cryptocurrencies onto the market to meet genuine demand. This is mirrored in the steadily rising prices of most cryptographic tokens, regardless of how volatile their prices are on a day-to-day basis. This delicate balancing act between hoarders, speculators, and spenders ensures a flourishing and healthy cryptocurrency market, implying that crypto tokens as an asset class are

already serving as money, among other things.

Chapter 2
Ethereum

In a nutshell, open-source blockchain networks like Ethereum and Bitcoin are software kits that let you create an economic system replete with account management and a native exchange unit that can be transferred between accounts. It's similar to the board game Monopoly. These native units of exchange are referred to as coins, tokens, or cryptocurrencies, but they are the same as tokens in any other system: they are a type of money that can only be used within that system.

Blockchains function similarly to mesh networks or local area networks (LANs); they are simply linked to other "peer" computers running the same software. When you wish to make one of these peer-to-peer (P2P) networks accessible through a web browser, you'll need to utilize specific software libraries like Web3.js to connect an application's front end (the graphical user interface you see in a browser) to its back end (through JavaScript APIs) (the blockchain). You may take this concept even farther in Ethereum by constructing financial contracts with other Ethereum users. Smart contracts, as you can see, are financial contracts.

Smart contracts in Ethereum are written in the Solidity programming language. Many developers flocked to Ethereum because of its Turing completeness, but its ability to store state is even more significant. According to a simple concept in computing, a stateful system can notice information changes and remember them across time. Consider a computer that doesn't have a hard disk; you wouldn't be able to do anything with it. It'd be like a

calculator, with the contents of its memory being ephemeral. The ability to build future interactions between users under specific conditions is a valuable addition to a blockchain. It enables programmers to add the control flow to cryptocurrency transaction programming. This is the most significant distinction between Ethereum and Bitcoin, but as you will see, it is far from the only one.

All transactions in Bitcoin are completed as quickly as feasible. Due to Bitcoin's lack of statefulness, transactions must be completed all at once. As envisioned by Bitcoin's creators, the blockchain was a distributed transaction record that kept track of everyone in the network's bitcoin balances. A comparable approach is made expandable in a standardized way in Ethereum.

Second, this common scripting language makes it easier for blockchains that utilize the Ethereum protocol to share data, allowing groups of people who use different blockchains to share data and value.

Ethereum (ETH)	Ethereum Classic (ETC)
• Controlled by the Ethereum Foundation (EF), a centralized authority • Blockchain state modifications can take place in the interests of EF related companies	• Controlled by a distributed community dedicated to the principles of openness, • Neutrality and immutability of the blockchain • Free from human intervention

Ethereum vs. Ethereum Classic

These Bitcoin governance issues were anticipated and addressed ahead of time by an 18-year-old prodigy named Vitalik Buterin in his 2013 whitepaper, "Ethereum White Paper: A Next-Generation Smart Contract & Decentralized Application Platform."

Instead of trying to fix Bitcoin, he came up with a whole new platform called Ethereum. The Ethereum network has a token (coin) named ether, but the general public still refers to Ethereum. On the exchanges, the symbol currently is ETH.

Bitcoin is like a restricted computer with only certain functions. Ethereum is like a full-purpose computer and was designed looking ten years ahead. The Ethereum network executes smart contracts better than the Bitcoin network does. Ethereum was designed as a platform upon which other coins/tokens can be set up to operate as a DAPP (Decentralized Application), which is a piece of software consisting of a user interface (UI) and a decentralized back-end, typically making use of the Ethereum blockchain and smart contracts. This use-case gives the Ethereum network a tremendous advantage. However, they have also had their share of hiccups.

The Ethereum network experienced a hard fork in 2016. The Ethereum network of miners split due to a significant theft from a group known as "The DAO," short for Distributed Autonomous Organization. The DAO raised

USD 150 million in ether (at the time) and was hacked, and a large number of their Ether coins were stolen.

What began as an attempt to rescue investor funds in this high-profile project ended up causing a schism that effectively split the Ethereum community. They held a vote, and most participants agreed that they wanted to change Ethereum's code to get the funds back to each investor and away from the attacker.

Those holding onto the original design retained the system as "Ethereum Classic" (ETC). Those miners who adopted the new software process brought the brand name "Ethereum" (ETH) because Vitalik Buterin and the other founders of the Ethereum network were part of this group.

This resulted in users now having access to two slightly different versions of the platform – Ethereum, the 'official version of the blockchain maintained by its original developers, and Ethereum Classic, an 'alternative' blockchain (but with the original design) maintained by a wholly new team.

In other words, 'Ethereum Classic' is the original blockchain where funds were never returned to Ether owners who lost funds in the hacking of The DAO. The current Ethereum, by contrast, is a parallel version of the blockchain that took measures to make the massive hoard of stolen funds unusable on their network.

Regardless of this unique one-off event, the Ethereum network is solid in its design and used as a platform by others. Many new tokens/coins are being developed on the Ethereum network using the "ERC-20" token standard. As central governments and state governments pass their Virtual Currency Regulation Acts, the number of businesses using these tokens/coins

could begin to avalanche.

Once the virtual coin concept goes mainstream, an increasing number of specialty design firms are expected to integrate more functionality with traditional commerce. For example, retailers like Walmart could use secure unforgeable coupon tokens to replace paper coupons. These will most likely be developed on the Ethereum and Ethereum Classic networks.

Since many of the tokens/coins being developed on the two Ethereum networks have strong use- cases, they can become (and in some cases have already become) more valuable than the underlying Ethereum/Ethereum Classic coins themselves. Over the next several years, the price of ETH/ETC or any one of these other coins/tokens could far exceed Bitcoin in value due to their speed of execution and usefulness.

Some speculators believe that every major company will eventually have to use blockchains for their transactions because it is the only way to ensure that they do not have a hacker in their system or a rogue employee.

Many platforms and banks already accept Ethereum in exchange for US Dollars, so any token created by a company could be exchanged for Ethereum, which can then be exchanged for USD, meaning that Ethereum could also function as a reserve currency with significant differences between it and Bitcoin. The designers of the Ethereum network have not set an official limit to the total number of Ethereum coins that can be issued, as there is a portion of coins that are being consumed as "gas" to complete transactions. Initially, they made the mistake of giving too many coins to stakeholders and designers and did not reserve enough coins for miners. Miners do not have any contractual agreements, and if people stop mining, the system shuts

down. If there is no compensation for serving as the network's backbone, the miners will start pointing their rigs to other coins.

This is why several proposals modify the system by changing how coins are issued, used, and consumed. Currently, the Ethereum community is discussing a shift to a "proof of stake" model instead of a "proof-of-work" model. If this proposal goes forward and there is no unanimous vote among network nodes, this might result in another fork in the Ethereum network.

Ethereum Chains and Movement

Bitcoin, as we know it today, is not the only large-scale Bitcoin software implementation. Litecoin, for example, and dozens of other cryptocurrencies employ customized versions of the Bitcoin software. Ethereum was constructed on the notion that copycats are inevitable, that there will be multiple blockchains, and that there will need to be a set of protocols in place to allow them to communicate.

Ethereum designers tacitly take the position that cryptocurrency will not be one decentralized system with a drastically different outlook than the Bitcoin creators if it exists in the future. Instead, it will be a distributed network of decentralized systems that will make it simple to create and implement various cryptographic tokens of value, each with its own set of functions and meanings.

If you work in financial services or studied economics, you've undoubtedly concluded that Bitcoin is essentially a global Ponzi scheme after browsing Google for more information. Let's get this over with. The market for bitcoins determines the worth of a bitcoin. Yes, certain bitcoin-holding companies have secured local money transmitter licenses and will exchange your bitcoins for US dollars, Euros, gold, or other fiat currencies. On the other hand, these organizations are for-profit corporations that demand fees and could go out of business at any time.

As a result, Bitcoin and similar networks are only susceptible to the extent that no "redeemer of last resort," that is, no trusted (governmental or corporate) organization that you can trust to redeem your bitcoins or ether for US dollars in the future. The only way to convert bitcoins to something of

actual value, short of paying a private money changer, is to join an online exchange and trade the coins for fiat currency, thus finding another buyer.

The Ethereum network moves ether tokens in the same way that the Bitcoin network moves bitcoin tokens. As you'll see, ether functions differently than bitcoin and is better classified as a crypto commodity rather than a currency. Let's look at how Ethereum's economics relate to the underlying technology.

Ether: Currency and Commodity

It’s a popular misconception that bitcoin isn’t backed by anything, and this is correct. Modern fiat currencies, on the other hand, are not supported by anything. But they’re not the same: a fiat currency is owned by default by everyone paying taxes or purchasing government bonds because the government backs it. Some foreign commodity sales such as oil and gas are also denominated in dollars, giving customers even another reason to own dollars.

The adoption of cryptocurrencies continues to be a difficulty. These digital tokens are now utilized as a quick, secure, public payment layer on top of the existing fiat money system; they are an experimental deployment that may one day grow to replace the centralized payments networking technology used by firms such as Visa and MasterCard.

Governments and private institutional investors are beginning to develop substantial markets for financial products and services denominated in cryptocurrencies, which opens up unique opportunities. Central banks may adopt the technique. Barbados is the only country with a digital currency based on Bitcoin software at the time of writing. Seven others are actively looking into the possibility.

Blockout History

True, Bitcoin and Ethereum add a layer of complexity—economics—to software development. In some ways, though, they are simpler; dealing with decentralized protocols is analogous to working with computers in the 1970s. Individuals might rent time on these machines from a university or organization that owned one, and they were massive and expensive shared resources. The Ethereum network works as a single huge computer that runs programs in lockstep; it's a machine that's "virtualized" by a network of other machines. The Ethereum Virtual Machine (EVM) can be considered a shared, ownerless computer because it comprises numerous private computers.

The process of persuading the Ethereum community of node operators to upgrade to a new version of the Ethereum software is known as hard forking. The core development team cannot simply push changes to the network. They entail a political persuasion and exposition procedure. This ownerless setup aims to maximize uptime and security while reducing the incentive for deception.

Chaos in the Crypto World

At this moment, your thoughts may be racing, and you may be worried. Never fear, though: anyone looking into blockchain development for the first time is likely to be overwhelmed. It’s a new technology, things are evolving quickly, and decentralized system knowledge is scarce.

Nobody knows what will happen next, but the technology is working —to the tune of USD billions of dollars, almost the whole market capitalization of all cryptocurrencies. Retailers large and small, online and offline, are starting to accept digital currency as payment.

So don’t stop here, even if you’ve never programmed before. The Ethereum project is designed with new developers in mind, providing you with the tools to construct previously unimagined solutions to age-old issues.

Protocol’s Power

The application layer is present in today’s technological industry: it’s where all the user data resides. Multibillion-dollar corporations like Google, Facebook, and Twitter have invested heavily in infrastructure to support multinational user communities. All of this is on top of TCP/IP (Transmission Control Protocol/Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), and a few other protocols.

The application layer in Ethereum, like Bitcoin, is thinner, at least so far, because the protocol provides so much. In truth, many Bitcoin-based businesses are only thin coatings on top of what is already a highly efficient payment system.

As a result, the Bitcoin startup boom that so many VCs predicted just five or six years ago never materialized. Instead, the Bitcoin sector began to consolidate swiftly. 10 However, in less than a decade, the market valuation of Bitcoin as a network has risen to about $19 billion. Ethereum has a market capitalization of around $1 billion. This is an unheard-of, lightning-fast method for launching a new network protocol.

Traditional web applications are expensive because they must be designed to retain and communicate user data and hence must have methods to separate bad actors from eliciting trust. Many private data centers are hidden behind layers of razor wire and bomb-resistant landscaping. When a secure decentralized network surpasses the security provided by these layers of private infrastructure, online business owners experience substantially cheaper overhead costs, which they may pass on to customers to challenge

legacy players. Apps and services built on the blockchain are disruptive because of their security and how cost-effective they may be to operate at scale.

Trustless System: A Build

When you learn the Solidity programming language, you'll quickly wonder what kinds of programs you can develop, and that's when the actual learning curve begins. The projects in this book aim to demonstrate how and where blockchains may improve or automate end-user experiences in various enterprises and enable new products and services. You'll discover how trustless distributed or semi-distributed systems can improve, benefit, or expand the financial products and services we know today, which have evolved over a thousand years of trial and error. "Not requiring faith that counterparties would operate honestly and without failure, hence immune to fraud and other counterparty risks" is the definition of trustless in this context. There is already some good information available on the Internet for software developers interested in learning more about Ethereum and Solidity.

Commerce: An Addition

Solidity code can be used on the backend of an application to add micropayments, user accounts, and functionality to even the most basic computer systems without third-party libraries or significant programming skills.

Consider that the mixing instructions function only costs a few pennies in ether to run. Your smart contract would call the mixing instructions function and instruct the user how to create the cake when the price of the cake recipe is removed from the user's Ethereum wallet balance —which takes a few seconds on average. All of this can be done without using authentication, payment APIs, accounts, credit cards, complicated web forms, or any other standard e-commerce development duties. That software package mentioned earlier, Web3.js, is all your JavaScript application needs to interface with the worldwide public Ethereum chain.

Content Creation

So far, we've focused on ether's monetary applications, but the main course illustrates another vital area of Ethereum's potential: intellectual property, licensing, and content royalties. Selling content on the web or through applications today necessitates interacting with big distributors such as Apple, Google, and Amazon, which impose strict laws on digital content sales and charge exorbitant fees.

Ethereum enables microtransactions in which a user pays only $0.25 for a recipe, a sum that would be impossible to pay through fee-laden credit-card networks. The price fluctuation of the ether token is a difficulty for content creators doing business this way today. Still, as you'll see in the following chapters, these issues will be resolved as the network grows.

Source Data

Where is the user data stored since the network protocol gives so much functionality out of the box, and this is a distributed system? Here's a quick rundown of how transactions are logged in Ethereum: Every network node has a copy of everything. All transactions in Ethereum are stored on the blockchain, which is a canonical history of state changes stored on every Ethereum node.

When you pay for computing time on the Ethereum network, you're also paying for the cost of processing the transaction as well as the cost of storing the data in your smart contract. (If your contract shrinks after it's completed, you'll get a partial refund in the form of a decreased transaction charge.) That data will be added in the next block as soon as your smart contract is executed and the fees are paid from your ether balance. Any node on the Ethereum network can query the database locally because all nodes must retain a complete state database of all contracts. You're paying attention if this sounds unscalable. Versions 1.5 and 2.0 of Ethereum describe a roadmap for addressing this scalability issue.

Mining 101

Machines can join the Ethereum network at any time and begin validating transactions since a distributed system has no one owner. Mining is the term for this procedure. Mining nodes consult to reach an agreement on the order in which transactions should be processed across the system, which is required to keep track of everyone’s account balances in real-time, even as many transactions flow through the network. Because this process uses electricity, which is expensive, miners are compensated for each block they mine around five ether.

Ether and Electricity Prices

For mining and running scripts on the network, miners are compensated in ether. One of the aspects that lend ether, as a crypto commodity, its intrinsic worth is the cost of electricity spent by servers running on the Ethereum network. This means that someone paid actual money to their electricity company to run their mining equipment. Mining rigs, which use many graphics cards to increase their odds of completing a block and being paid, can cost $100 to $300 per month in electricity, depending on local rates.

Mining is an essential part of both Bitcoin and Ethereum, and it operates similarly in both networks in theory, with a few exceptions. Ethereum has also changed the paradigm in this area, particularly in terms of ether issuance.

Browser vs. Wallet or Keychain

Mist is sometimes referred to as a wallet, a phrase taken from the Bitcoin community. What is the meaning of the term “wallet” in the context of Bitcoin? Wallet applications do not retain your money, but they do allow you to send and receive payments. When you install these apps on your phone, you’ll be given cryptographic keys that let you read and write data to a decentralized database. The wallet is the phrase we came up with, although the keychain is a better metaphor.

Sample contracts may be tested using fake ether using mist and the Ethereum command-line tools, ensuring that you don’t lose any actual money while troubleshooting. And suppose you’ve worked with newer development tools. In that case, it’s an excellent place to start for non-technical learners because it challenges them to learn about networking and low-level computer systems to construct a simple demo app.

Advantages of Ethereum

Ethereum is well suited to the development of pure software economic systems. In other words, it’s business logic software that allows people (users) to transfer money (data signifying value) around at the same speed and scale as data. Not like the commercial banking system, which has a three-to-seven-day floating period. Or the costs charged by companies like Visa, MasterCard, and PayPal. It is relatively straightforward to pay hundreds of thousands of people in hundreds of countries modest amounts every few minutes with a simple Ethereum application. At the same time, in the legacy banking system, you’d need an entire payroll department working overtime to rebalance your account ledgers and deal with cross-border difficulties continually. You’d need a whole payroll department working overtime.

If you’ve seen the Ethereum commercial, you’ve undoubtedly got a somewhat more dramatic idea of what this software can do. Here’s a list of wishful thinking regarding Ethereum and the blockchain in general, along with some clear and popular rebuttals.

“No downtime, censorship, or third-party interference.”

The way the codebase is managed may appear perplexing at first if you’re not accustomed to opening source development. Even though a small number of core engineers created the Ethereum protocol, now that the network is up and running, various stakeholders must collaborate to improve its performance. These so-called hard forks will become less practical and required as the network grows, and therefore less frequent. Keep in mind that the Ethereum network is still in its early stages. It’s up and running right now, but it won’t be finished until 2019. The Ethereum Foundation, a Swiss non-profit, has been bestowed with funds to continue development.

“A secure, free, and open platform for the Internet of Things”

Many smart contracts may be executed by machines, according to the theory. Let’s imagine you’re wandering around a new neighborhood and lose your phone service. Your phone may automatically “rent” time from a neighboring femtocell in another network and pay a small price to the router, all without your approval. A router-authored smart contract, akin to a service-level agreement (SLA) that can move money when you agree to it, may include price and speed as variables.

“Enabling transparent governance for communities and businesses.”

Okay, this one is a little tricky: transparent businesses are a foregone conclusion. However, decentralized autonomous businesses (also known as DAOs or DACs) are likely a long way off. The term employed in this book is a decentralized organization, or DO, which appears to be the industry’s consensus. It isn’t easy to make progress in this area. All of the same tricks that have plagued democracies for centuries may be found in cryptography governance. Is it true that one vote equals one wallet address? Who gets a wallet address, after all? Do the wealthy have the upper hand if a coin represents a vote? That discussion is generally outside the scope of this book. Still, anyone trying to sell you on the idea of fully autonomous organizations, whether corporate or governmental, is likely to have a bridge you’re interested in.

“Handles user authentication and secure payments for you, as well as messaging and even decentralized storage”

This will be fully realized once Ethereum has progressed further along with its roadmap. When you connect to the Ethereum blockchain, you get user identification and safe payments out of the box. Still, peer-to-peer communication and decentralized storage (a young section of blockchain software enterprises) are now only available through third-party integrations. However, these aspects are slated for inclusion in the Ethereum roadmap under the titles Swarm and Whisper. Both are accessible in restricted experimental forms right now.

“No need to sign up and pay for application host; the world’s first zero-infrastructure platform”

Technically correct, but time is money, and as we examine hosting and deployment, it will become evident that in this new software world, free and straightforward may be mutually exclusive notions.

State of Smart Contract Development Today

There are now only a few Solidity development sample projects available. There won't be much competition if you want to deploy a complete end-user application. However, the blockchain's greatest strength lies in developing applications that allow users to conduct transactions such as purchasing, selling, licensing, trading, streaming, and so on. This means that people must be holding ether or a native coin associated with your project. The liquidity of a native coin refers to its circulation and availability. High liquidity can also have network effects, resulting in more stable currency values. To gain the benefits of liquidity, many enterprising developers may strive to bootstrap their coins into circulation. This is precisely how the EVM and ether function. When the Ethereum Foundation was founded in 2014, it was crowdfunded to the tune of $18 million. Bitcoin contributions were repaid in ether, and a community was established.

Copycat Coins

Bitcoin clones that use the Bitcoin codebase are known as alt-coins. There are genuine motivations for launching an alt-coin; they aren’t constantly attempting to force a user base to exist. Many of the core concepts of Bitcoin are retained in Ethereum, yet it can be regarded as an entirely new network because its key components are different.

Project Funding

By selling early access to a product or service to prospective users, crowdfunding is one way for entrepreneurs to avoid the pain and expense of live beta-testing and fundraising. This is known as a token launch in the crypto world. Because the word “initial coin offering” (ICO) sounds similar to the term “initial public offering” on Wall Street, some companies have embraced it (IPO). However, because tokens may not always represent equity, this concept is deceptive. This is true for both ether and bitcoins, which aren’t backed by anything.

The Ethereum network also functions as a completely redundant distributed database, with copies stored on each node. That means you can rely on your application to make a call when a specific condition is met, even if the situation occurs decades later and the nodes have all changed.

Newbie Programmers: A Heads Up

Knowing how existing monetary, banking, and insurance systems work will be extremely useful when conceptualizing Ethereum applications. It’s even better if you can create that with some technical understanding. So, even if you’re not a programmer and have no plans to become one, pay attention to the portions about code. It will assist you in grasping the boundaries of what is conceivable. Learning Ethereum development may be easier and more intuitive than learning web development from the ground up in several ways.

Ethereum: Free and Open Source

Ethereum may be forked and copied in other systems while maintaining compatibility. Coins may be able to be transferred from one chain to another in the future. Even though this is not a simple process, academic articles on how it can be done already appear. For those who aren't programmers, it's worth remembering that free and open source are not synonymous. Open source is a software development process, while freedom is a societal notion. "When we term software free, we mean that it respects the users' core freedoms: the right to run it, to study and edit it, and to redistribute copies with or without changes," according to the GNU Foundation.

In a nutshell, Ethereum aims to provide a system that allows economic models to be tested and proven. Solidity appears to be on track to become the de facto language for such models for the time being, as long as they are executed on a global virtual machine like the EVM.

Private and Public Chains

Because anyone can fork the Ethereum project, instead of working on the public chain, you can “create your own Ethereum.” This is known as a private blockchain, and it reflects a duplication of effort by the Ethereum development community, similar to Bitcoin’s alt-coins.

Private chains are often a bad way to do things for a startup product or service, as you’ll see by the end of this book, but that hasn’t stopped some companies from trying to build one. Rather than recreating the wheel, entrepreneurs should build on top of the public Ethereum blockchain.

As you can see, the public chain dedicates a significant amount of computer power to security, making it relatively simple for small businesses to build large-scale secure online services. However, because the public Ethereum blockchain is now completely public, some businesses may prefer to maintain sensitive transactions on a private chain linked to the public. The deployment is characterized as a permissioned blockchain in an enterprise software setting, where corporate stakeholders are given special rights and privileges to read and write to the company chain. Wallet addresses for permission blockchains are often issued by a trusted third party who confirms your consent to enter the system, similar to how a security pass permits you to transact inside an office building. The public chain could be compared to a city park or other public area using the same concept.

You can do the following in both public and private Ethereum chains:

- Ether is sent and received.
- Smart contracts should be written

- Create programs that can be proven to be fair.
- Create your ether-based token.

Each is described in the following subsections.

Send and Receive Ether

You can transmit and receive ether. However, private ether is a worthless scrip on a private chain. Mobile wallet apps are also available on the App Store for iOS and Google Play for Android. To convert dollars for ether, you must first sign up for a cryptocurrency exchange or purchase via a commercial money transmitter like Coinbase. Most consumers simply buy bitcoins (which are more widely available in ATM form and through the LocalBitcoins.com cash dealer network) and then convert them to ether using an exchange or a crypto money-changing service ShapeShift.io.

Write Smart Contracts

Even if they include many variables or extend far into the future and across national borders, you can govern payments and transfers between accounts (and even between other contracts). The genuine potential here is determined by how unstoppable the public chain is, determined by who participates, and how many bad actors enter the system. On the other hand, private chains may provide the same capabilities to groups with resources, but only privately.

Create Provable Fair Applications

It is highly critical to provide provably fair applications for gaming and gambling. Expect points to be introduced into video games and virtual reality games that represent real money and can be spent in the real world.

Launch Your Token

In practical terms, creating your token is similar to creating a user account system. You can build a sub currency for use in a private transaction ledger that is only available to you and your private group but uses the public chain in all other ways, avoiding the need to fork or maintain your network of mining equipment using an Ethereum token contract. For most developers and companies, this is a more convenient and superior strategy.

The Promise of Decentralized Databases

A blockchain has a schema, much like any other database: rules establish, constrain, and enforce relationships between entities. Motives to break or alter these relationships can be found in various industries, leading to bribery and corruption and making blockchain's trustless properties even more appealing to businesses than previous generations of software and networking. Shared read/write access generates considerable complexity in all databases. Depending on where the database is physically situated, machines worldwide may experience variable latency, resulting in certain write operations arriving out of order. This becomes considerably more challenging when multiple parties are expected to share a database equitably, such as a collection of corporations joining an industry trade group. Large firms have found it prohibitively expensive to enable shared read/write status with other organizations, and consumer data leakage is now all too prevalent.

Today, corporate IT groups have figured out how to make these systems mostly perform as expected. However, when they grow in size, the potential for fraud becomes too great for some unscrupulous actors to ignore.

What’s Next: New Ways of Working

Thousands of Wells Fargo bank employees were fired in September 2016 for tampering with account databases to inflate sales figures and trigger bonuses meant to reward salespeople who opened new accounts. 15 The cost of those errors in judgment, as well as the expense of developing software that can prevent administrators from making erroneous modifications, will be tremendous. Ethereum offers businesses and consumers a new way to connect in a more secure environment than the application data layer on the HTTP web.

CHAPTER 3
The Mist Browser

Ethereum can refer to both the Ethereum protocol and the Ethereum network created by computers that use the protocol. You can upload smart contracts to the network by running a node. All you need is a wallet app for your computer or smartphone to transfer and receive cryptocurrency.

The Mist browser is the most helpful, as it is a user-friendly wallet that can perform some of the functions of a complete node, such as executing smart contracts. The mist will eventually be able to view whole web-app-like programs with Ethereum backends; that’s why it’s called a browser. Don’t be deceived by mist's ease of use. It can now be used to send and receive the ether coin. But, like an App Store, it might become a distribution hub for consumer and enterprise software programs tomorrow.

Wallets as a Computing Metaphor

Wallets are software apps that store your keys to the EVM on your PC or mobile device. These keys are associated with a specific account, which is identified by a lengthy account address. Your name or any other personal information is not stored in your Ethereum account. They use a pseudonym. Anyone can create an account by connecting to the Ethereum network with any Ethereum client (Mist). You have complete freedom to produce as many as you want.

You were presumably prompted to establish an account if you had already downloaded an Ethereum wallet or entire node on your computer or phone. The wallet application most likely also required you to generate a password to encrypt your keys. As you may expect, these keys are crucial for transmitting and receiving ether.

Let’s start with your account address, also known as a public key. Your public key is linked to a private key that grants account access. This private key should be kept private and not made public. In both Bitcoin and Ethereum, long hexadecimal addresses are used to represent accounts. The raw hexadecimal address in the Bitcoin protocol is encoded in base 58 with a built-in version number and checksum, yet it appears precisely like an Ethereum address below.

You must disclose to the sender your address to get ether or bitcoins, which is why it’s called a public key. These strings, of course, aren’t noteworthy. You might be wondering what the jumbled alphanumeric mess means if you’re new to programming. As experienced programmers may already know, asymmetric key cryptography includes these public and

private keys.

Ether Address

Why are account addresses supposed to be public and are even listed on some people's websites, such as long, obscure strings? Why can't we have usernames only?

The answer is that you will most likely construct plain-English usernames soon, but they will behave today more like top-level domain names. A decentralized network registrar will rent you a name, which will go to your actual account address, similar to how today's top-level domains do. Several Ethereum network initiatives are in the works that will someday imitate the conveniences of today's HTTP Web as we know it.

The network in the EVM uses asymmetric cryptography to generate and recognize valid Ethereum addresses, as well as to "digitally sign" transactions. Asymmetric cryptography is used in secure communications to encrypt private messages to remain unreadable even if opponents intercept them. The premise is the same in blockchain; it's a means to ensure that messages (in the form of EVM transaction requests) are sent by the correct address holder and not by a third party seeking to steal their cash.

Where Is My Ether?

It’s vital to keep in mind that ether isn’t confined to any machine or program. Any machine running an Ethereum node or wallet can check your ether balance and send or receive ether. Never fear if the machine on which your Mist wallet is stored is destroyed: all you need is your private key to access your ether from another node. However, if you give someone your private keys, they can access the EVM and withdraw your money without your knowledge. Anyone possessing your private key is you in the eyes of the network.

The EVM has no means of knowing which node you’ll generate a transaction from because it’s a global computer. Ethereum, unlike today’s online apps, does not look for a “trusted” computer; it has no way of distinguishing your phone from any other phone. Consider how anyone with your debit card number and four-digit pin can access your account through a bank ATM system.

Losing your phone or computer to theft or destruction does not imply that you will lose your money if the following conditions are met:

- You’ve made a copy of your private key.
- You didn’t provide anyone else with your private key.

Copying and pasting a private key into a text file and putting it on a USB stick is all it takes to back it up. Alternatively, you may write it down on paper. More private-key backup options will be discussed later in this chapter.

The Bank Teller Metaphor

In some ways, utilizing a wallet or full node is similar to taking control of your money at the bank teller's desk, in the sense that a bank teller is in charge of a node within the bank's computer system that can perform transactions in a worldwide database, not in the sense that you can obtain physical currency. A teller is in charge of the bank's database linked to other banks' databases.

A paper check is a written order for the bank teller to perform a transaction using the bank's computer system in traditional banking. The check has your account number and routing number printed on it. For the time being, it's simply necessary to mention that taking your paper check, converting it to an electronic transaction, sending the transaction to another party, and then updating the balances of both parties requires a large number of people (and a lot of processing power. The old banking system is completely replaced with an algorithmic consensus engine running on a peer-to-peer computer network—a jumble of human and computer processes—in cryptocurrencies. Transactions are settled and cleared on the network within seconds (or minutes in the case of bitcoin) of being digitally signed and broadcast by a node. As a result, "the settlement is the trade" in a cryptocurrency transaction.

Assets in Cryptocurrency

Cryptocurrencies are distinct from the centralized fiat currency utilized by traditional banks. Your tokens are virtual, and the blockchain network keeps track of your balance (and with that of everyone else who owns ether). Although some third parties have manufactured “collectible” coins preloaded with cryptocurrency, there is no ether or bitcoin currency.

Any online business or organization that offers to handle, store, or act as a custodian of ether, bitcoins, or any other cryptocurrency should be avoided at all costs. Distributed public systems provide the advantage of removing counterparties from transactions and allowing entities to transact on a peer-to-peer basis. The key is that you can keep these assets safe without the help of a custodian. We do, however, live in a fiat money world. Even if cryptocurrencies are the way, it’s possible that a transitional period of many years or more could occur. People will have both a cryptocurrency wallet and a regular bank account. Use no wallet or online service that stores your private keys on your behalf. Apps that save your private keys on your smartphone are the only ones to use.

Visualizing Ethereum Transactions

Imagine a paper transaction ledger that can be synchronized with other paper transaction ledgers across the world. This is the ideal way for new Ethereum programmers to comprehend the concept of a blockchain.

When a wallet application attempts to make a database change, the nearest Ethereum node detects the change and propagates it throughout the network. All transactions are eventually recorded on each ledger. In theory, this operates similarly to John Isaac Hawkins' polygraph machine, which was patented in 1803. Although its name is often used to refer to so-called lie-detecting technologies, this was the first "copy machine." The blockchain, like the polygraph, is a system that allows a large number of "machines" to change the state of a ledger in a near-simultaneous manner. In Bitcoin and Ethereum, the technological innovation lies in the fact that these state changes can come in out of order, owing to network latency, and the network can reconcile them into a single ledger

As mentioned previously, your address is sometimes called your public key, but a better metaphor would be a lockbox with a unique serial number. The private key is the only thing in this whole system named sensibly: it unlocks your account and allows you to move ether out.

What is ether, exactly? It's merely a balance in your account. When you send and receive either, nothing is sent or received. In the EVM, when one account increases, the system makes sure it's because another account has sent a payment and thus decreased the same amount. It's a closed system. It's practically impossible to give yourself free ether, or at least it wouldn't be worth the costs you'd incur trying to falsify the ledger. Ethereum uses

financial incentives and disincentives for security.

Breaking with Banking History

The issuance method of the Ethereum protocol, which will be explored later, is one of the most intriguing aspects of the system. For the time being, it's just vital to note that, like Bitcoin, no single person can produce more ether. This trait contrasts sharply with the history of financial markets and central bankers over the previous 400 years, which reads like a history of large-scale con artists.

Entrepreneurs and scammers (then known as stock projectors) have been selling equity in legitimate and illegitimate companies since the late 17th century's stock-jobbing days in London's Exchange Alley. When the stock price rose, they would often covertly issue new shares to themselves and their associates, a practice known as "watering the stock" in the United States in the nineteenth century.

Speculating on stocks became a popular sport for people of all ages and backgrounds on both sides of the Atlantic. The modern stock markets were established, complete with protocols and counterparties to function as trusted intermediaries. Despite the banking laws enacted during the Great Depression, dishonest businesspeople continued to carve out secret stock pools or unload their shares without the public's knowledge—only to have the business collapse after they had taken their money.

Few speculative bubbles in modern history have wiped out as much money and progress as the United States stock market crash of 1929. Similar depressive events in the United States and Europe (particularly the Panic of 1873–1879) were produced by someone meddling with the base quantity of money, shares, or bonds in a significant marketplace (either central banks or

investors).

Trust to Encryption

We have skimmed over any explanation of cryptography instead of focusing on the impact of crypto-networks. However, there's something odd about a secure network made up of a bunch of strangers' PCs cooperating. What makes you think that a single bad apple can't attack the network and take everyone's ether? To address that question, keep in mind that a blockchain employs the following procedures:

- Asymmetric cryptography
- Cryptographic hashing
- Peer-to-peer distributed computing

Let's take a quick look at the first item on this list: asymmetric cryptography, sometimes known as public-key cryptography. We'll take a slight detour here to understand better how a public network can be secure.

Asymmetric cryptography is a means of exchanging secure communications over a network when neither the sender nor the recipient trusts the communication channel. In the case of the EVM, those messages are transactions being signed and sent to the network to change the state of some of its accounts. It's called "asymmetric" because each party has a pair of two different but mathematically related keys.

Public-key cryptography was developed for wartime communications, and when used properly, can be highly secure. Unlike symmetric-key cryptographic, public vital cryptographic communications

don’t require a secure channel between parties. This is essential in Bitcoin and Ethereum because any computer running the protocol can join the network without any vetting. However, the computational complexity involved in encrypting data makes it useful only for small data objects, like the alphanumeric string that becomes your private key. This is why encryption must be used sparingly.

At a high level, it can be said that Ethereum uses encryption to validate and verify that any changes made to account balances in the EVM are legitimate and that no account has been increased (or decreased) erroneously. If you’re new to computer science, the very mechanism of encryption might be hazy.

Symmetric Encryption: A process by which a snippet of plain text, usually held in a document, is smashed together with a shorter data string called a key to produce a ciphertext output. This output can be reversed or decrypted by the party that receives it, so long as they also have that same key. Trying to decode the message without the key would be, computationally speaking, immensely time-consuming and expensive—so much so that some kinds of encryption are considered practically unbreakable, even with substantial computing resources.

Asymmetric encryption: This way of encrypting information requires the program to issue two keys simultaneously, one that is public and one that you keep private. The public key is public in the sense that it can be displayed on your website or social media profile, similar to an e-mail

address. (When communicating, parties can use one anothers' public keys to encrypt information, as described below.)

Secure Messaging: In our first example, Alice uses Bob's public key to encrypt a message. When he receives the ciphertext, he can decrypt it using his matching private key, ensuring that only Bob can read the message. This is called secure messaging. But it leaves a dangerous possibility open: anyone could send Bob a message claiming to be Alice. How does he know that Alice is the real sender of the message?

Secure and Signed Messaging: If Alice wanted to assure Bob that she is the true sender, she would do things differently. First, she would take her plaintext message and encrypt it using her private key. Then, she would encrypt it again using Bob's public key. When Bob receives the message, he decrypts it first using his private key, but he's still left with ciphertext. He must decrypt it again using Alice's public key. This second layer of encryption assures him that Alice is indeed the sender because presumably, nobody has Alice's private key but Alice. This is known as "secure and signed" messaging. If Alice were to encrypt her plaintext using her private key, anyone with her public key could decrypt it. This is known as an "open message format" because anyone can decrypt it while proving the sender's identity.

Digital signature: For maximum security, Alice would take another step: she would hash the plaintext of her message and attach it along with it. She would then encrypt this bundle with her private key and again

with Bob’s public key. When Bob receives and decrypts the ciphertext, he can run Alice’s plaintext message through the same hashing algorithm Alice used. If for some reason, the fingerprint of the message turns out differently, then it means the actual message text was damaged or altered en route.

Mist Installation: System Requirements

Most users will opt for the Mist browser, but this section lists other tools that developers may find just as enjoyable. The mist makes it easy to send and receive ether. It also contains an interface for executing smart contracts quickly and easily. Mist runs well on a modern computer with at least 2 GB of RAM and 30 GB of hard disk space free. For lower-performing machines, try the MetaMask Chrome extension. It’s described later in this section.

Tools for Developers

Developers will want to check out these three tools in addition to mist:

• **MetaMask Chrome extension** (valid for everyone)
• **Geth** (useful for intermediate developers)
• **Parity** (useful for advanced developers)

The Chrome extension MetaMask is the simplest way to get up and running with Ethereum. It lets you execute smart contracts and transactions right in your browser without needing a full Ethereum node. MetaMask has the power to create accounts and to send and receive ether. You can download MetaMask from the Google Chrome Add-Ons menu or navigate to the project URL at https://metamask.io/.

MetaMask does not download the entire blockchain to your computer, nor can it mine transactions and earn ether. However, these are minor drawbacks for users just looking to get up and running with Ethereum quickly. It was built by Aaron Davis (a.k.a. Kumavis) of ConsenSys, an Ethereum development and consulting company whose free tools you'll frequently encounter in this nascent Ethereum blockchain space. ConsenSys is a 60-person Ethereum venture studio and consulting company in Brooklyn, NY, run by Ethereum project co-founder Joseph Lubin. It was funded in part by development grants (DEVgrants) from the Ethereum Foundation. These grants are open to anyone working on an Ethereum project and do not require the project creator to give up any equity.

Working with Messages and Transactions

In both Ethereum, transactions refer to state changes in the distributed database (in the blockchain). Transactions change account balances within the EVMMessages are data objects transmitted back and forth between smart contracts across the network. Still, they do not always result in modifications to the chain. For example, if one contract checks the balance of another.

Transactions Change State

In Ethereum, a transaction is a piece of data with a cryptographic signature entered into the blockchain and thus stored on every node in the network. Every transaction sends a message to accomplish this state change, but messages are also delivered by EVM code. The parties' messages are private, and they are not recorded on the blockchain.

Editing a Global Database

Blockchain networks like Ethereum are touted as immutable because once a transaction is written to the globally shared database, it cannot be reversed by any other transaction. In modern payments terminology, this is known as a system without chargebacks.

A chargeback in North American payment channels is defined as the forcible return of funds to an account holder initiated by the issuing bank of the instrument. Because Ethereum has no central issuing authority, no one can appeal to it if you mickey a transaction. Presently, the only way to roll back a transaction is a state fork, which requires all nodes on the network to agree to revert a transaction manually. This is an extremely difficult and unlikely scenario reserved for network-wide attacks of one form or another.

The reason for this transaction model is security. Compare sending cryptocurrency from one account to the other to the process of writing a conventional paper check. In the latter example, your bank receives news of the outgoing transaction from your account. The bank first checks your balance to see whether you have the funds to pay the amount you endorsed on the check; if you don't, the depositor's bank does not increase the deposit account. Instead, you are issued a fee for writing a bad check.

Transactions in the Ethereum network work similarly. The system ensures that the outgoing amount from one account is always added to the destination account. If the destination account can't be accessed for some reason—say because the cryptographic signature is not valid—then the source account doesn't have its balance decremented, and thus funds are not lost. In Ethereum, externally-generated transactions are always signed

cryptographically with the keys of the sender and the recipient, making it straightforward to ensure that bad actors can’t create transactions, and money can’t be lost just because of a miskeyed address.

Blockchain: A Revelation

So far, we've carefully avoided breaking down the concept of blocks and focused on how transactions are initiated. Next, we'll discuss how those transactions are cleared and settled by the network. A heartbeat is a period during which a particular amount of blood is moved through an animal's body, while a block is a unit of time that spans a given number of transactions. Transaction data is captured throughout that time, and when the unit of time expires, the next block begins. The blockchain is a representation of the history of state changes in the EVM's network database. To paraphrase the Ethereum documentation:

The blocks on the blockchain represent time units, and the blockchain preserves the whole history of states at the discrete-time points defined by the blocks.

Smart contracts may be uploaded to the network in a given block but may not send any messages or transactions until a much later block.

Paying for Transactions

When a human sends a transaction, the EVM requires a small fee to process the transaction. This works similarly for the uploading of smart contracts: users must pay for the EVM's computational effort to expend running each contract. Compelling users potentially lower the risk of inefficient never-ending programs being performed to pay for transactions on the EVM. These expenses are calculated in a unit known as gas.

Gas can be thought of as a metric that indicates how many steps the EVM will have to take to accomplish the transaction's instructions. If the transaction is simply one person giving money to another, the transaction cost will be low because only a few computing steps are required. The price for a sophisticated smart contract, on the other hand, will be higher because the EVM will have to utilize its global resources to run the contract's Solidity code and figure out what transactions to perform as a result.

Transaction senders are required to include a gas limit that says how much they're willing to pay to have their transaction executed. Full nodes on the network which are mining, or securing the network for pay, provide the hardware for these many transactions to be collated, validated, cleared, settled, and stored within the blockchain. Thus they receive the transaction fees a user pays when they send ether to a friend or executes a smart contract. Miners who execute the transaction collect the cost, so an implicit market process is at play. Whether or not a transaction will be done is determined by the quantity of gas the sender is willing to spend. If the total number of steps in a transaction exceeds the gas allotted for that transaction, all actions are rolled back, and the transaction is not completed. If a user sends a transaction with a transaction fee that is too low, it will be executed slowly or not at all.

For context, every operation costs some gas; most operations cost 1 unit of gas. A complex transaction can cost hundreds of units of gas. However, in dollar terms, this adds up to very little.

Understanding Denominations

Like fiat currencies, ether balances and values have standardized denominations for small units. All ether balances are typically denominated in ether, and remainders are denominated in wei. For example, 10.234 ether = 10,234,000,000,000,000,000 wei.

If you think of ether as dollars, wei are like dimes, quarters, pennies, and nickels. Figure 1 details the Wei denominations.

Unit	Wei Value	Number of Wei
Wei	1 wei	1
Kwei (babbage)	1^3 wei	1,000
Mwei (lovelace)	1^6 wei	1,000,000
Gwei (shannon)	1^9 wei	1,000,000,000
Microether (szabo)	1^{12} wei	1,000,000,000,000
Milliether (finney)	1^{15} wei	1,000,000,000,000,000
Ether	1^{18} wei	1,000,000,000,000,000,000

Figure 1. Wei Denominations

Getting Ether

Converting bitcoins to ether in the Mist wallet, as detailed earlier in this chapter, is the simplest way to obtain ether. You can earn either by mining, but as mentioned previously, this requires initial setup; you can’t mine from within mist unless it’s on the test net. If you’d like to buy ether with fiat currency, such as US dollars, you need to do so on an exchange or with a licensed money transmitter.

Anonymity in Cryptocurrency

Bitcoins and ether are not anonymous payment instruments. Anyone who knows your public key can look on the blockchain and see the dates and amounts of transactions coming in and out of your account. From this data, they might be able to put together a pattern of transactions from which they could deduce your activities. Federal authorities are already using machine-learning transactions to decode spending patterns on dark market sites such as AlphaBay.

Newbies generally conflate anonymity, secrecy, and privacy in cryptocurrency, sometimes with disastrous ends. Bitcoin and Ethereum addresses are pseudonymous by nature; they're not linked to your real name or information. But every transaction you send is public, in the sense that anyone can see the transaction on the blockchain. This is why public blockchains are touted for transparency; if you know someone's public key, you can look up all their transactions.

Data within smart contracts themselves are encoded but not encrypted. Encryption is used only to hash large datasets and verify transaction senders and recipients. However, you can encrypt data yourself before putting it into an Ethereum smart contract if you'd like to use the public Ethereum chains privately. Every Ethereum transaction leaves room for an extra payload of text labeled Input Data. Don't be tempted to store secret things here for safekeeping unless you plan to encrypt them. Even then, it is generally a bad idea to store strings such as passwords or account pin numbers on the Ethereum blockchain because it is public and can never be removed. Anyone can explore a blockchain such as Ethereum by using a web-accessible application known as a blockchain explorer.

CHAPTER 4
Ethereum Virtual Machine

All transactions are local and executed in relative synchrony on each network node in the EVM, which is a single, global 256-bit "computer." It's a virtual machine made up of several tiny computers that can be accessed from anywhere in the world. This giant computer, which anyone with a node or wallet application can access, makes it simple to move arbitrarily large amounts of value (money) nearly instantly. Although anyone can use this global virtual machine, nobody can create counterfeit money inside it or transfer funds without permission.

Suppose it seems wasteful to have the entire EVM, all those nodes, replicating the duplicate transactions and slavishly maintaining the same state among thousands of individual computers. In that case, it’s essential to have a proper basis for comparison for how financial services IT works today. The EVM is a paragon of simplicity and efficiency by comparison! More importantly, all that work isn’t for naught. As you’ll see in this chapter, it’s the evidence of this work that secures the network.

The Central Bank Network of Yesterday

Today, corporations, insurers, universities, and other large institutions spend incredible amounts of money building and maintaining software services and IT for their employees and all their lines of business. Large commercial banks reconcile their various inflows and outflows with their architecture, policy, codebase, databases, and infrastructure layers. Of course, all of this is on top of the Fedwire, the Federal Reserve's real-time gross settlement system, or RTGS.

All Federal Reserve member banks use the Fedwire to settle final payments in electronic US dollars. Any qualified state-chartered bank may become a member of the system by buying shares in it. Fedwire is owned and administered by the 12 Federal Reserve Banks, and while it does charge fees, it is not a profit-making enterprise. This system processes incredible amounts of US dollars every day—trillions upon trillions. It has some great features, too: there’s an overdraft system covering all existing and approved accounts, and the system is famously reliable, even for remittances overseas. It's been around for almost a century in some form or another.

As you can imagine, maintaining the security and reliability of the Fedwire software is extremely expensive. Yet, the cost of building and keeping layers on top of an RTGS is higher still, owing to its security requirements. Ultimately, these costs are passed on to corporations who use commercial banks in the form of fees. Those companies have their own IT infrastructure costs. In the aggregate, these costs ultimately drive up prices and fees for consumers.

Virtual Machines 101

If you were unfamiliar with virtual machines at the outset of this book, you've probably gathered by now that a virtual machine (VM), in the Ethereum context, is one giant global computer composed of constituent nodes, which are themselves computers too. Generally speaking, a virtual machine is an emulation of a computer system by another computer system. These emulations are based on the same computer architectures as the target of their emulation. Still, they're usually reproducing that architecture on different hardware than it may have been intended for. Virtual machines can be created with hardware, software, or both. In the case of Ethereum, it's both. Rather than securely network thousands of discrete machines, as with Fedwire, Ethereum takes the approach of securely operating one vast machine that can encompass the whole Earth.

The Role of the Ethereum Protocol in Banking

We might now speculate on whether blockchain-based systems are suitable for use by sovereign central banks or whether they can truly replace them. It's much more likely that central banks themselves will adopt the technology. The commercial banks are certainly interested in this.

The Fedwire system is a settlement system with a user experience tailored to state-chartered banks and their operators. It makes little or no concern for the end-user of a retail bank. For example, that's the job of the retail bank. Software developers will recognize Fedwire as a "platform for banks." The bank chooses to build on top of Fedwire (the customer experience, the online banking tools, the brick-and-mortar branches, the financial products, the cross-selling) and distinguishes it from other banks on the Fedwire system.

Anyone Can Make a Banking Platform

Ethereum is far more generalized. It allows anyone to spin up a network with as good or better security and reliability than Fedwire and with the ability to make secure value transfers nearly instantly. But this is only where Ethereum starts. Developers can build any sort of financial products or business logic they want on top of this secure ledger, with automated and immutable scripts, without needing to pay the overheads dumped on them by the traditional centralized hosting and banking infrastructure.

But does it scale to the speed and size of a system like Fedwire? The answer is, yes, it can, but this will take several years. There are no direct or fixed limits neither for transaction sizes or block sizes. In Bitcoin, the size of the block is limited to 1MB, which works out to about seven transactions per second. In Ethereum, these limits increase and decrease by demand and network capacity. However, this does not mean that blocks can be unlimited in size. Recall that units of work in the Ethereum network are priced in gas. Thus, larger, more complex smart contracts cost more gas to store and execute. The maximum number of gas spent per block is variable, but there is a maximum. Theoretically, one significant transaction could consume the entire gas limit of a single block. But if there is a continuous demand for higher gas limits, the system will increase the gas limit per block in increments of 0.09 percent.

What does this mean for the financial services industry? Certainly not doom, but perhaps some unexpected competition. The impact could be an unbundling of banking services into ever smaller brands as the public Ethereum chain scales and can process more transactions, faster and faster. Laura Shin, author, and host of the blockchain-centric podcast Unchained,

interviewed Adam Ludwin of San Francisco blockchain startup Chain in 2016 and wrote this:

In terms of who owns the network, under the existing system, if you go to Chase to deposit $50 in cash, Chase holds that money on its network, which the Federal Reserve issued. Fedwire, the present mechanism for electronically settling payments between member banks, might be reconstructed on a blockchain, with banks holding keys to make transfers rather than banks administering the network, according to Ludwin.

What the EVM Does

By now, the EVM may be coming into focus: a generalized, secure, ownerless virtual machine that offers cheap Fedwire-like functionality with a bunch of other magic on top. How exactly does it do this?

The EVM can run arbitrary computers written in the Solidity language. These programs will always produce the same output with the same underlying state changes given a particular input. This makes Solidity programs fully deterministic and guaranteed to execute, provided you've paid enough for the transaction. Solidity programs are capable of expressing all tasks accomplishable by computers, making them theoretically Turing complete. That means that the entire distributed network, every node, performs every program executed on the platform. When one user uploads a smart contract through their Ethereum node, it is included in the latest block and propagated around the network, stored on every other node in the network.

As we've discussed already, each node in the EVM's job is to run the same code as part of the block processing protocol. The nodes go through the block they are processed and run any code enclosed within the transactions. Each node does this independently; it is not only highly parallelized but highly redundant.

Despite all appearances, this is an efficient way to balance a global ledger reliably. It's vital to recall how much money, electricity, and human energy each bank spends to put together its own unique IT system or cocktail of systems for each of its business lines. In an Ethereum-based banking system, all users (whether corporations or customers) get direct access to the

same Fedwire-like system at no cost, with the ability to program transactions. Because the protocol is free and open-source, anyone can fire up a node and connect. Unfortunately, the preceding explanation of the Fedwire system is often left out of cryptocurrency discussions, despite being necessary context to understanding the benefits of large public blockchains.

EVM Applications Are Called Smart Contracts

The EVM is also a runtime environment for small programs that can be executed via a network from the perspective of a software developer.

Smart Contracts

Rather than bore you with the etymology of this word, let’s clear up one thing: in this context, the contract refers to a specific kind of contract: a financial contract, also known more colloquially as a derivative or option. Financial contracts are agreements to buy and sell at some point in the future, usually at a specified price. In the Ethereum context, smart contracts are agreements between accounts to render ether (a payment) transfer when certain conditions are met. These contracts are “smart” because a machine executes them, and the assets (ether or other tokens) are moved automatically. These contracts could be enforced even hundreds of years after they’ve been written, assuming the network is still running then—and even if many bad actors try to interfere. The EVM is sandboxed and free from interference, isolated from other networks, making it impossible for a party to back out of a smart contract. In practical terms, smart contracts are empowered to hold assets (ether or other tokens) in escrow and move them when the contract terms are met.

The EVM Runs Bytecode

The EVM has its language, the EVM bytecode, to which your smart contracts compile. Solidity, a high-level language, is compiled into bytecode and uploaded onto the Ethereum blockchain by using a client application such as the Mist browser or a full node.

Understanding State Machines

The EVM, as we've discussed several times so far, is a state machine. Instead of simply defining this concept and moving on, let's take a moment to discuss exactly what a computer is before moving on to how Ethereum advances the idea.

Digital vs. Analog

Foundational to the concept of a stateful computer is the idea of a switch on or off. The 1s and 0s, always referred to as the lingua franca of machines, refer to arrays of metaphorical switches. To speak, put in a particular configuration to code for specific letters, numbers, or other keyboard symbols. All of the symbols on a keyboard (and more) can be represented with just eight switches, which is why computing memory is stacked in multiples of eight. The so-called character code for a comma, for example, is 0010 1100.

Statements

When considered by themselves, individual snippets of code fall broadly into two buckets: expressions and statements. Expressions are used to evaluate a particular condition; statements are used to write information into the computer’s memory. Together, expressions and statements let computers modify a database in a predictable way when specific conditions are met. This is the crux of automation, and it’s the reason we find computers so useful.

Statements can evaluate as true or false, and depending on the code. This binary outcome can add, remove, or alter information within one of the computer’s many, many memory addresses. The clear distinction between true and false, yes and no, on and off, is what allows computers to make decisions instead of humans safely.

Data’s Role in State

Every time you change data in a computer’s memory, you can think of its zillions of internal switches (most of them virtualized in the same way we discussed earlier in this chapter) as being in a slightly different configuration. The state generally refers to the present condition of the system: the objective series of information changes across various memory addresses of the machine that led to the current contents of its memory.

It's critical to understand the difference between an attribute and a state. The state is something that can change easily and predictably. Let’s use the example of a car. Repainting a car is hard work, but it can be done. Paint color is an example of an attribute. In pseudocode, you might say the following about a car:

bodyColor = red

In computer programming, this is called a key/value pair. The key, bodyColor, has a value assigned to it, which is red. To change the value of this key, your code makes a new statement of the value to be something else:

bodyColor = green

And now your car has been repainted. It has a new color value. Now let’s say you instruct the computer that the color of this car will change frequently. In other words, you make the car’s paint a variable. Well, it can be said that the variable (in this case, the color) can have a state, which is a value that changes. But an individual matter, such as green, has no form; green is green.

An odometer provides another example of a variable with a changeable state. The odometer's value might be 1,000, a number that itself has no form; it's just a number. Soon, the state of the odometer will change to a new value (1,001), but that will happen only if the cockpit of the car expresses commands that cause the motor and transmission to change state from neutral to first gear so on.

Working familiarity with the concept of state transition will help nonprogrammers gain insight into the challenging problems incumbent in the design of decentralized systems.

How the Guts of the EVM Work

If this is your first interaction with a computer's internals, keep in mind that a laptop is never truly "at rest" as long as it's turned on. The computer itself is running a state function, constantly checking for changes to its state. It’s like an overeager intern who wonders thousands of times per second if any new work has landed on his desk.

When new instructions are triggered, the computer runs code and may write new data to its memory. It’s important to note that each state change must be based on the last state change; a computer doesn’t just toss information into memory addresses willy-nilly. Should something go wrong —let’s say one of these instructions isn’t mathematically possible—the machine's state will become invalid, and the program will exit or stop. The entire system may crash.

Programs that constantly check for a specific condition are known as loops in programming because they continue to run (to loop) until the specified condition is met. The EVM runs a loop continuously that attempts to execute whatever instructions are at the current program counter (whatever program is “on deck” to be processed). The program counter works like a delicatessen queue: each program takes a number and waits its turn.

This loop has a few jobs: it calculates the cost of gas for each instruction, and it uses memory, if necessary, to execute the transaction if the preamble calculation succeeds. This loop repeats until the VM either finishes running all the code on deck, throws an exception or error, or that transaction is rolled back.

The EVM Constantly Checks for Transactions

State machines (machines with memory) can be thought of as beings who never sleep. As a state machine, the EVM has a constant history of all transactions within their memory banks, leading back to the very first transaction. Unlike people, who have to deal with imperfect memory, a computer's state (as it exists today) is the specific outcome of every single state-change that has taken place inside that machine since it was first switched on.

The latest version of the machine's state can be said to be this machine's canonical "truth" about reality as it stands right now. In Ethereum, this truth deals with account balances and the series of transactions that make your balance whatever it is today.

Creating a Common Machine Narrative of What Happened

Transactions, therefore, represent a kind of machine narrative—a computationally good arc between one state and another. As Gavin Wood's Ethereum Yellow Paper says:

> *There exist far more invalid state changes than valid state changes. Invalid state changes might, e.g., reduce an account balance without an equal and opposite increase elsewhere. A proper state transition comes about through a transaction.*

As time advances, the system (as in Bitcoin) seeks to create a trustworthy history for ensuring that each subsequent state change is legitimate and not an instruction inserted by a bad actor.

Cryptographic Hashing: Hash Functions

Generally speaking, the purpose of hash functions, in the context of a blockchain, is to compare large datasets quickly and evaluate whether their contents are similar. A oneway algorithm processes the entire block's transactions into 32 bytes of data—a hash or string of letters and numbers containing no discernible information about the transactions within. The hash creates an unmistakable signature for a block, allowing the next block to build on top of it. Unlike the ciphertext that results from encryption, which can be decrypted, the result of a hash cannot be "un-hashed."

Blocks: The History of State Changes

Transactions and state changes on the Ethereum network are divided into blocks, which are then hashed. Before the following canonical block can be placed on the "top" of it, each block is inspected and confirmed. In this way, nodes on the network do not need to individually evaluate the trustworthiness of every single block in the history of the Ethereum network, simply to compute the present balances of the accounts on the network. They merely verify that its “parent block” is the most recent canonical block. They do this quickly by looking to see that the new block contains the correct hash of its parent’s transactions and state.

All the blocks strung together, including the genesis block, an honorific describing the first block the network mined after coming online, is called the blockchain. You will hear the blockchain referred to as a distributed ledger or distributed ledger technology (DLT) in some circles. Ledger is an accurate description, as the chain contains every transaction in the network's history, making it effectively a giant, balanced book of accounts. However, most so-called digital ledgers do not use proof of work to secure the network, as Bitcoin and Ethereum do.

Understanding Block Time

In Bitcoin, a block is 10 minutes. This so-called block time is derived from constants hardcoded into Bitcoin's issuance scheme, with a total of 21 million coins to be released from 2009 to 2024 and rewards halving every four years.

Block time in Ethereum is independent of the ether issuance schedule. On the other hand, block time is a variable kept as low as possible to guarantee that transactions are confirmed as rapidly as possible. It averages about 15 seconds as of this writing. Ethereum's shorter block time is the beneficiary of blockchain research done after the launch of Bitcoin, which showed that shorter block times were not only technically feasible but desirable in many ways. However, faster block times do have some drawbacks that are explored more thoroughly in Chapter.

The Drawbacks of Short Blocks

It’s important to note that Bitcoin’s long confirmation times make retail commerce and other practical applications difficult. When blocks are shorter and transactions move faster, the user experience is better. However, more temporary blocks and faster transactions make it more likely that a given node will get the order of transactions wrong because it may not have heard about some transactions originating from far away (or heard about them late). To compensate for this, the miners who find valid blocks but not the winning block are paid a reduced fee as consolation. In Ethereum, these blocks are called Uncles

“Solo Node” Blockchain

In theory, you could reconcile changes from many nodes with a single computer: a centralized server processing the order of transactions. Indeed, web applications such as Google Docs have sophisticated real-time engines that help them deal with conflicting changes made by multiple users, some of whom may be on faster connections than others, and still others who may be editing a document offline. It’s even possible to use the Ethereum protocol with a single machine. It will process your transactions just fine, as long as one or more nodes are mining on the chain. But if someone knocks that machine offline, your chain is inaccessible, and transactions stop going through. For this reason, despite Ethereum being free and open software, the necessity for many, many nodes to create a resilient network causes developers to converge and work (for the most part) as one community on a small number of public chains.

Distributed Security

The distributed nature of the Ethereum Virtual Machine, and the fact that it is composed of many nodes around the world, means that it must be purpose-built to solve the diffmatching problem that can arise when there are many near-simultaneous changes to the same database, from many users, all over the world.

Indeed, solving this problem in a verifiable and trustworthy way is the purpose of the EVM and the Bitcoin virtual machine. The EVM’s resilience and security arise from the large number of machines mining on the network, incentivized by the earning of fees denominated in ether or bitcoins.

Mining's Place in the State Transition Function

Mining is the process of using computational work to nominate a block—that miner's version of recent transaction history—as the canonical block for this, the most recent block on the chain. Mining achieves the consensus required to make valid state changes, and the miners are paid for contributing to the consensus building. This is how ether and bitcoin are "created."

Recall that each time a new block is created, it is downloaded, processed, and validated by a node on the network. During processing, each node executes all the transactions contained therein. For each transaction in a block, the EVM performs the following:

1. Check whether the transaction is in the proper format. Does it have the correct number of values? Is the signature valid? Does the nonce—a transaction counter—on the transaction match the nonce on each account? If any of these are not on the list, return an error.

2. Calculate the transaction fee by multiplying the amount of work required (represented by STARTGAS, as you'll see in table 3-1) by the gas price. Then deduct the fee from the user's account balance, and increment the sender's nonce (transaction counter). If there's not enough ether in the account, return an error.

3. Initialize the gas payment; from this point forward, take off a certain amount of gas per byte processed in the transaction.

4. Transfer the value of the transaction—the amount being sent—to the receiving account. If the receiving account doesn't exist yet, it will be

created. (Offline Ethereum nodes can generate addresses, so the network may not hear of a given address until a transaction occurs.) If the receiving address is a contract address, run the contract's code. This continues either until the code finishes executing or the gas payment runs out.

5. If the sending account doesn't have enough ether to complete the transaction or the gas runs out, all changes from this transaction are rolled back. A caveat is the fees, which still go to the miner and are not refunded.

6. Refund gas to the sender and transfer any fees connected with the gas used to the miner if the transaction fails for any other reason.

Renting Time on the EVM

As you may be gathering, the EVM is a rather deliberate machine, albeit far more trustworthy and reliable than any network we have today. To prevent the system from getting meaningless spam contracts, there must be a fee associated with each instruction the EVM executes. Every time an instruction executes, an internal counter keeps track of the fees incurred, charged to the user. Each time the user initiates a transaction, that user's wallet reserves a small portion (selected by the user) to pay these fees.

After a node broadcasts a transaction to the network—say, Bob transfers Alice some ether from his computer—the network propagates the transaction so that all nodes can include it in the most recent block.

Gas 101

Gas is a unit of work used to measure how computationally expensive an Ethereum operation will be. Gas costs are paid with small amounts of ether. The purpose of gas is twofold. First, it guarantees a prepaid reward for the miners that execute code and secure the network, even if the execution fails for some reason. Second, it works around the halting problem and ensures that performance can’t go on longer than the time it prepaid for. Gas is a unit of work; it’s not a sub currency, and you can’t hold or hoard it. It simply measures how much effort each step of a transaction will be in computational terms.

To be able to pay for gas costs, you simply need to add ether to your account. You don’t have to acquire it separately; there is no gas token. Every operation possible on the EVM has an associated gas cost.

Gas: Importance

Gas costs ensure that computation time on the network is appropriately priced. This works differently in Bitcoin, where the fee is based on the transaction size in kilobytes. Because Solidity code can be arbitrarily complex, a short snippet of instructions could generate a lot of computational work, whereas a long snippet could generate less. That’s why fees in the EVM are based on the amount of work being done, not on the size of the transaction.

Because ether is traded publicly on cryptocurrency exchanges, it is subject to speculative periods of inflation and deflation. Using the gas unit of account for computational work is helpful because it separates computation from the highly volatile price of the ether token.

Fees as Regulation

Networks such as Bitcoin and Ethereum use economic incentives and disincentives to render specific attack vectors moot. Fees fall into the category of disincentive. To begin with, it’s essential to recognize that the operation of an Ethereum node represents some risk. There’s the cost of the hardware, plus the time and energy of the operator, and the network’s worth of downloading and verifying the proof of work and the block header. Thus it makes sense that a transaction fee is put in place to prevent pranksters from wasting the network’s capacity.

Blocks that consume excessive amounts of gas are a significant danger in Ethereum. They can take a long time to propagate because of their sheer size. How the system adapts to the demands of users, who may have legitimate uses for large smart contracts, will become clear later on in this chapter and Chapter 6. The protocol helps cut off late blocks using various methodologies we’ll explore in Chapter 6 and places a floating cap on operations, which currently sits at 65,536 per block.

Gas Specifications

• Unfortunately, the term gas creates some confusion. Every transaction requires a STARTGAS value. This value is referred to as gas limit in the Yellow Paper and often just as gas in Geth and Web3.js.

• Every transaction also requires the user to specify a gas price.

• The amount stipulated in STARTGAS, multiplied by the gas price, is held in escrow while your transaction executes.

• If the gas price you offer for a transaction is too low, nodes won’t process your transaction, and it will sit unprocessed on the network.

• If your gas price is acceptable to the network, but the gas cost runs over what’s available in your wallet balance, the transaction fails and is rolled back; this failed transaction is recorded to the blockchain, and you get a refund of any STARTGAS not used in the transaction.

• Using excessive STARTGAS does not cause your transactions to be processed more quickly, and in some cases, may make your transaction less appealing to miners.

How Gas Relates to Scaling the System

If you send a computationally difficult set of instructions to the EVM, the only person this hurts is you. The work will spend your ether and stop when the ether you allocated to the transaction runs out. It does not affect anyone else's transactions. There is no method to jam the EVM without spending a significant amount of money on transaction fees. The gas price system serves as a de facto means of scalability. Miners have complete control over which transactions pay the highest fee rates, as well as the block gas limit. The gas limit sets the maximum amount of processing (and storage) that can be done per block. In this way, the price of computation on the EVM stays flexible and responsive to the demand of the system users and the costs incurred by the miners who do the vital work of processing transactions, maintaining hardware, and paying electricity bills.

Accounts, Transactions, and Messages

Externally Owned Accounts

An externally owned account (EOA) is also known as an account controlled by a pair of private keys, which a person or an external server may hold. These accounts cannot hold EVM codes. Characteristics of an EOA include the following:

- Contains a balance of ether and capable of sending transactions
- Controlled by the account’s private keys and has no code associated with it
- A key or value information database contained in each account (both 32-byte strings)

Contract Accounts

Humans do not control contract accounts. They store instructions and are activated by external accounts or other contract accounts. Contract accounts have the following characteristics:

- Maintain a healthy ether balance
- Keep some contract code in your head.
- Humans (sends a transaction) or other contracts (sends a message) can trigger it.
- When used correctly, it is capable of performing complex processes.
- Have a persistent state and the ability to call other contracts and have no owner after being released to the EVM
- A key or value information database contained in each account (both 32-byte strings)

Transactions and Messages

Transactions come from external accounts, which human users usually control. It's a way for an external account to submit instructions to the EVM to perform some operations. In other words, it's a way for an external account to get a message into the system. In computing terminology, a message is a chunk of data containing instructions. Programmers can think of messages as function calls.

A transaction in the EVM is a cryptographically signed data package storing a message (as described previously), which tells the EVM to transfer ether, create a new contract, trigger an existing one, or perform some calculation. Contract addresses can be the recipients of transactions, just like users with external accounts. Recall the discussion of cryptographic communication from Chapter 2. We discussed encrypted communications: a transaction is like a private communication between two users in an unsecured network who can "send" value to each other.

Characteristics of Transactions

Transactions contain the following:

- A recipient address; specifying no recipient (and attaching smart contract data) is the method for uploading new smart contracts. As you'll see, a contract address is returned so that the user knows where to access this contract in the future.

- A sender's signature

- A value field indicating the amount being transferred

- A message data field that is optional (if this is being sent to a contract address)

- A STARTGAS value that indicates how many computing steps the transaction is prepaid for.

- A GASPRICE value, representing the fee the sender is willing to pay for gas

Characteristics of Messages

A message is a chunk of data sent by a contract to another contract (never to or from a human). Messages are non-serializable virtual objects that reside solely in the EVM. When a miner is paid in the Ethereum network, this is accomplished through a message to increment the miner’s payment address; it does not constitute a transaction. A message is sent when the EVM runs a contract, and it executes the CALL or DELEGATECALL opcodes.

Messages are sent to other contract accounts, which in turn run the code enclosed in the message. Thus, contracts can have relationships with each other.

The following is part of a message:

- The message's sender address
- The message's recipient address
- The field of value
- an optional data field
- A STARTGAS number that sets a limit on how much gas the message can use.

CHAPTER 5
Smart Contracts and Tokens

Smart contracts, a nod to financial contracts, are small reusable code templates (in programming terms, classes) created in Solidity. Smart contracts are similar to online services for establishing financial derivatives, but with a few differences.

EVM as Back End

As they currently exist for the Web, iOS, macOS, Windows, Android, Linux, and so forth, software apps are typically discussed in two halves: the front and back end. The back end usually refers to the database and the logic around interacting with it, which (as you learned in Chapter 3) is where the program stores its information. The front end usually refers to the user's application: the interface with its various labels and controls. In software interface design, controls are the general term for the tiny buttons, sliders, dials, hearts, stars, thumbs-up icons, and any other little thing you can click to make something happen.

Modern-day web-enabled applications use a constellation of computers and servers. Most of them run some Linux version, which plays a vital role in a sometimes-fragile choreography of computers working together to deliver a “seamless” experience on your smartphone or computer.

Neither EVM nor the Bitcoin virtual machine is powerful today. The EVM will continue to get faster as the core developers iterate toward a faster block time; how that works will become more apparent in Chapter 6. The takeaway is that the EVM replaces the traditional application end of a conventionally hosted web or mobile application. Although the EVM itself is a fully-fledged computer, it is not yet a complete end-to-end platform capable of hosting HTML/CSS interfaces; the most valuable role it can play is as the back end to a distributed application.

Smart Contracts to Dapps

A smart contract is just a unit of functionality you upload to the EVM. The term distributed application, or dapp, typically describes a web- or smartphone-accessible front-end GUI application that uses the EVM as its back end. Unless it’s a very simple dapp, its back-end functionality will rely on several smart contracts.

Assets Backed by Anything

A valuable resource that you expect will provide you with a benefit or value in the future is referred to as an asset. Assets can include physical natural resources or abstract financial instruments, but by definition, the price of an asset should go up over time. (If it goes down, it is known as a depreciating asset.) It can be said that cryptocurrencies are assets backed by anything. What exactly this means will become apparent by the end of this chapter. Let’s look at an example next.

Bartering with Fiat Currency

Let’s say you are Alice, and you live in Japan. Assume that you are paid in Japanese yen and that the pricing of goods like rent, food, and essential services are also denominated in yen for this example. Now let’s say you want to pay someone in New York to do some translation work. His name is Bob. Bob, the translator, uses US dollars; he holds them as savings; he pays taxes in USD, too.

This creates a problem. For most people, foreign currency is not of much use, and exchanging it incurs high fees and risks of price slippage. Slippage refers to the price dropping before you have a chance to sell your lot. Bob doesn’t want yen, and Alice doesn’t hold any dollars.

Although this example uses fiat amounts of money, Alice and Bob may also have cabbage and glass beads to barter. Although indeed, one of them can drive to the nearest bureau of exchange, probably at an international airport, that’s not an economical solution. With cryptocurrency, they need only establish a conversion rate, or multiplier, between their local currency and the cryptocurrency and then convert the local price of the barter goods by using that multiplier. Whether they’re using paper money or glass beads isn’t relevant. For a trade to take place, they merely need to agree on a price.

Ether as Glass Beads

This example demonstrates one of the fundamental properties of ether and bitcoins: they are standard accounting units of value and simultaneously media of exchange themselves. Money also serves these functions, but in actuality, the medium of exchange (paper) is just a representation of value in some bank's ledger. Here, they are the same.

These standard account units essentially tabulate themselves and balance the entire ledger anytime a payment moves from one place to another. This is another advantage over the money of today, which, being inert, has no "awareness" of other funds in the system. As you may be imagining already, this makes smart contracts perfect for writing self-executing financial agreements.

A derivative contract is a financial "bet" between two or more parties made on the underlying asset's value. A derivative says that under certain conditions, Alice agrees to pay Bob a particular amount. The number of financial derivatives currently on Earth tops $1 quadrillion dollars.

Cryptocurrency Is a Measure of Time

Because crypto-assets and cryptocurrencies are impossible to counterfeit, this gives them an exciting property measure of time. Chapter 7 covers the issuance scheme of ether, but the point here is that these tokens are almost like the rings of a tree—their manufacture happens by a sophisticated process that cannot be “sped up.” As a result, while negotiating with someone from a different economy, it's simple to trust cryptocurrency prices because counterfeiting is impossible, no matter how wealthy or strong the entity you're dealing with is.

Cryptocurrencies are not redeemable by any central authority for gold or fiat currency. However, they are classified as property or currency in a handful of countries. Nevertheless, it can be said that cryptocurrency gets its price from the marketplace: they are worth whatever someone in the marketplace will pay. In contrast, this is a gold-backed currency redeemable from the local treasury or even a treasury bond. A government guarantees it will redeem for its fiat currency decades into the future.

Cryptocurrencies can be thought of as "assets backed by anything" due to their status as a decentralized digital means of exchange. It doesn’t matter whether you’re trading cattle, bananas, soybean futures, or private equities—the deal can be done in cryptocurrency. The only challenge is agreeing on a price.

Today, even if the buyer and seller agree to complete their transaction in cryptocurrency, it’s likely they will quickly sell the cryptocurrency for local fiat money to avoid price slippage. As the price of cryptocurrencies stabilizes, this will become less common. Prices become more stable as the

volume of transactions increases worldwide, and the markets for trading cryptocurrencies become deeper or more liquid.

Ether is similar to other cryptocurrencies such as bitcoins. In this regard, it does gain some intrinsic value from its usefulness in paying gas costs on the EVM. As discussed in Chapter 3, this makes ether more like a commodity such as oil or corn, which get their respective intrinsic values from their uses as fuel and food, respectively.

Asset Ownership and Civilization

The invention of money as a social construct is foundational to civilization. The pantheon of Great Human Ideas probably ranks among innovations such as animal domestication, geometry, and stone tools. Being highly susceptible to the network effect, money seems to evolve more slowly than other technologies. Because people prefer money that can be saved for long periods, retaining value far into the future, human societies aren’t exactly eager to jump to new media of exchange, lest their savings become worthless.

The concept of network effect describes how technologies become more valuable on an individual basis as their popularity grows and widens across geographical space. Being able to use bitcoins to buy retail goods worldwide is an example of its positive network effect. It makes trade possible everywhere you go. Savings, or surplus value, enables people to invest in the future. Whether 50,000 years ago or today, having extra food, fuel, or human labor at your disposal allows you to plan and take actions that use that surplus to facilitate even more enormous surpluses for future generations. An example is a community that expands its population after a bumper crop of food and collectively builds a dam to irrigate its fields, improving farming yields even further.

Your Pile of Savings = Reputation

People who accumulate savings in a particular form of money, whether gold, wampum, or US dollars, will reinvest for their future. Typically, people invest in the geographic areas where they and their families reside. This is known in economics as home bias. It is one way that humans achieve status in a community: by donating public works, leading constructive social movements, or providing large-scale employment.
Any organization does not guarantee Bitcoins and ether to be redeemable for anything at any point in the future. Thus, a family seeking to protect its inheritance might consider bitcoins or ether a poor choice for long-term savings. The same goes for other farsighted institutions such as charities, pension funds, trusts, and endowments.

Who knows if anyone will be using these networks in 50 years. By contrast, nation-states tend to stick around for centuries. When they issue fiat currency, they also raise armies to protect their economic systems; there is no such central power enforcing the use of bitcoins or ether. To make matters even less certain, computer networks, in general, haven’t been around long enough to know the lifespan of their utility, as compared to, say, governments, which have existed (in some form or another) for millennia and can last thousands of years.

Money, Tokens, and Reputation

Longevity is an asset's defining characteristic: the longer an item will increase in value and the more difficult it will be to counterfeit, the more desirable it will be. That’s why so many people store their wealth long-term in bonds and real estate.

The point of ramming home this reality is to think of bitcoins and ether as digital collectibles. As you’ll see, this is the most helpful approach when considering the many uses of smart contracts. After all, learning how to write programs for the EVM is just as challenging as figuring out what to build. And the long history of money gives us many clues as to what kind of novel business transactions or social constructs may be possible with this new asset class.

Much has been written on Ethereum's potential to bring the true potential of the Internet, particularly the Internet of Things, to bear. From the literature about Ethereum that’s already on the Web, it’s easy to imagine industrial or retail scenarios in which small computers can execute microtransactions. But this view limits us to transactions we already make today. The promise of the Ethereum and Bitcoin protocols is the introduction of new kinds of transactions and instruments.

Coins are Collectibles

Let's start with some anthropological background, courtesy of Nick Szabo, a cryptocurrency pioneer whose prolific web articles impacted many of today's cryptocurrency aficionados and cypherpunks.

Szabo wrote a paper in 2002 regarding the intersection of physical things and abstract value throughout human history. We were able to engage in larger, more intricate financial transactions because of these collectibles, he continued.

Collectibles were crucial in making these kinds of transactions possible for the first time. Collectibles augmented our large brains and language as solutions to the Prisoner's Dilemma that keeps almost all animals from cooperating via delayed reciprocation with nonkin.

If you don't have a reliable collectible to trade back and forth, you might not be willing to trade resources with anyone outside your extensive kin network. In larger nation-states, this does not bode well for harmonious coexistence.

The Function of Collectibles in Human Systems

Money's primary role is to track favors over time: it acts as a closed accounting system for a community to track favors owed and favors provided. As larger organizations strive to interact and collaborate, this becomes more useful. The essence of primal accounting is calculating favors with valuables. The value of these favors was eventually abstracted, leading to the development of generalized value instruments such as gold. This explains the modern-day link between affluence and self-esteem.

Ethereum and Bitcoin hit at the heart of tens of thousands-of-year-old problem: reputation-accounting is a normal, but imperfect, human behavior. Szabo goes on to say:

There are two types of inaccuracies that might affect reputational beliefs: errors in determining who did something and errors in estimating the worth or damages caused by that conduct. It is possible that every local clan member kept account of every other local clan member's favors in both Homo sapiens neanderthals and Homo sapiens, with the same big brain size... Both tracking and collections were utilized between clans within a tribe.

A private bank database is similar to two tribes within a tribe exchanging collectibles within a closed system. Alternatively, a private blockchain. According to Szabo,

Collectibles completely supplanted reputation as the enforcer of reciprocity between tribes. However, violence continued to play a significant part in upholding rights and was a high transaction cost that barred most types of commerce.

Just like the banks of today, human groups of yesteryear had trouble trading outside their accounting system. It's no surprise that there was so much bloodshed: the temptation to cheat is just too strong.

Early Counterfeiting

Inter-tribal trading was solved by using rare art objects: not just rare earth elements, but anything that was difficult to find or make from scratch. They couldn’t be just any set of beautiful things. They had to be rare or the result of expert craftsmanship, ensuring that each collectible represented a certain amount of human labor. The resulting collectible can be considered “proof of work” by the craftsman. As a result, we're back to the original concept: bitcoins and ether as a time store. As Szabo puts it:

It had to have particular useful features, such as the ability to be worn securely, compactness for concealment or burial, and unforgivable costliness. The transfer beneficiary had to verify the costliness using many of the same techniques that collectors use today to value treasures.

Jewelry and Art as Money

There’s perhaps nothing more essential to human economic progress as a reliable set of collectibles that can be used as money. This is because money facilitates cooperation. Szabo goes so far as to say that cooperation is our defining adaptive feature at the group level:

Most large animals on the earth are now scared of projectiles, which is an adaptation to only one predator species.

Yes, that’s us, the tool-creating apes who hunt like wolves and live in social colonies like termites! In a sense, modern cryptocurrencies are a super-lubricant for our sophisticated human cooperative systems because they introduce the building blocks of an immutable system of account that can span the geography of the entire world.

The Step toward Banknotes

Money, reputation, and social standing have always been intertwined. Understandably, primitive riches were wearable, such as gold jewelry or diamond-studded crowns. However, when a community becomes wealthy, everyone gains access to a small amount of gold, followed by a little more and then a little more. A rising tide provides new markets for products and services, allowing the wealthiest people to enjoy themselves while simultaneously displaying their social position.

When it becomes too much to wear and carry, people start competing on abstractions like product brand names or their children's school. By this point in a developing society, there’s enough wealth stocked up in the banks that individual account holders begin trading in banknotes. Martin Armstrong, an economist, is the best person to explain how this works. He declares:

The distinction between banknotes and deposit receipts issued by goldsmiths was a simple one. If a deposit receipt was payable to the "carrier" rather than an account, it was converted into a banknote. As a result, Paterson's Bank of England effectively generated circulating notes via de facto since its receipts were receivable to the "carrier," thereby establishing circulating "banknotes" when such an instrument was not provided for.

Bitcoin revised this relationship only slightly by creating bearer accounts; whoever has the password and private key of an account is by default the owner. Bitcoin addresses, like Ethereum addresses, do not belong to specific people. They are created pseudonymously.

Ether is like the issuance of banknotes that are also redeemable for computing time on the EVM.

Platforms for High-Value Digital Collectibles

In a digital context, a reliable store of time has incredible potential as a platform for digital collectibles: valuable items that can be displayed, worn, or hung in one’s personal space—either online or in real life—and that are not possible to knock off, nor easily stolen from their rightful owner. The majority of people associate the Internet of Things with sensor motes, self-diagnosing industrial equipment, and self-driving cars. The Internet of Value, a euphemism is referring to blockchain technologies, one of the many metaphors used to represent Ethereum and Bitcoin conceptually. However, rather than thinking abstractly, consider the possibility in terms of valuable artwork, jewelry, fashion, or luxury goods that resemble today's but have verifiable provenance and ownership maintained on a blockchain.

The ownership, worth, and provenance of a tangible object may never be "lost" in the future if the blockchain where it was inventoried is still active. In 100 years, there will be no Antiques Roadshow on television. (We could even write a smart contract to take that bet!)

Tokens Area Category of Smart Contract

Generally speaking, the Ethereum protocol prides itself on being featureless, which is one reason that tokens (as a concept) overlap so heavily with smart contracts (as a concept). Tokens are just one application of smart contract functionality on the EVM. That said, Ethereum does make provisions for one common use-case of smart contracts, which is a sub currency, a.k.a. token. The Ethereum developers have included an easy-to-use template inside the Mist wallet for swiftly establishing your tokens to make it simple to get started. Presumably, other templates for common smart contracts will follow. But at present, the one we get out of the box is creating a custom unit of value that can be passed around, alongside ether, within the EVM.

If you were to phrase the user-friendly token-making progress as an elevator pitch for its value proposition to users, it would be something like this: “ultra-secure digital monetary system with automatic ledger balancing delivered as a service.”

Tokens as Social Contracts

Tokens are sometimes called coins, and these are also smart contracts. But tokens themselves (like all forms of money) can also be seen as social contracts or agreements between user groups. In plain English, the implicit understanding of a group using a token would be as follows: “We all agree this token is money in our community.” It’s also a tacit agreement not to counterfeit, undermining the system. The closest thing we have to a social contract in software form today is probably the end-user license agreements or EULAs that users sign when they create an account on services such as Facebook, Twitter, iTunes, or Gmail. This agreement usually includes language barring activities such as spamming other users, which would degrade the user experience.

Thinking this way allows us to imagine how our digital media and digital goods today might become digital collectibles that are discussed, marketed, sold, and displayed inside the social networks of the future, in which online artifacts like selfies and podcasts can be sold, licensed, or rented for fees of arbitrary size.

Tokens are a Great First App

When making a token, consider that it is only as valuable as the community using it believes it will be. Thus, it is far easier to launch a token into an existing community that already trades using some kind of money or scrip. When making a token, consider that it is only as valuable as the community using it believes it will be. Thus, it is far easier to launch a token into an existing community that already trades using some kind of money or scrip.

In Ethereum, tokens exist within, and rely upon, the public blockchain: you can create a sub currency of ether, but ether will always remain the privileged token with which miners and gas costs are paid. If you want a purely independent blockchain network, you can create your private blockchain and be completely disconnected from the main Ethereum chain. Making a sub currency is more straightforward and will satisfy most use cases for curious developers.

CHAPTER 6
Mining Ether

The Ethereum network obtains consensus about the sequencing of transactions in a particular time through mining, which allows the EVM to make valid state transitions. It is important because it is the process by which consensus is reached in the system and by which ether is created. Ethereum, like Bitcoin, employs mining to gain agreement, but due to its capacity to execute smart contracts, the way things work in Ethereum is a little different.

In the pursuit of something as idealistic as the EVM, a world computer that anyone can use, it's essential to be realistic about how its advantages and disadvantages are assessed. At this point, you may be wondering whether such a sophisticated (or complicated) network can ever succeed. However, like many of our modern-day systems, it's essential to understand the problem being solved. The solutions may change, and indeed the Ethereum protocol (like the Bitcoin protocol) will adapt and change over time. But the issue of trust in human societies is persistent.

It's also important to recall that the creators of decentralized networks are cryptographers at heart, interested in one goal: creating an accessible, trustless world computer that is much harder to destroy than create. To quote Vitalik Buterin:

Cryptography is unique in the twenty-first century since it is one of the only domains where adversarial conflict favors the defender strongly. To some

extent, crypto-economics is a continuation of cypherpunk ideology, which is basically about harnessing this valuable imbalance to create a world that better maintains individual autonomy rather than simply maintaining the integrity and secrecy of private correspondence. Systems that claim to be ideological heirs to the cypherpunk philosophy should have this essential quality. They should be substantially more expensive to destroy or disrupt than they are to use and maintain. The "cypherpunk mentality" isn't just about ideas; designing systems that are easier to defend than attack is plain good engineering.

Ether’s Source

Ether is considered the native token of Ethereum because it gets created out of thin air during the mining process as payment for mining work performed by computers. Because mining is computationally intensive, it can generate high electricity costs for your home or office. Miners take their rewards seriously.

Mining rewards are accomplished through an account balance increase programmed into the EVM’s state transition function. They are payable to whichever random miner finds a block. (To mine, you need to pass the mining method an Ethereum address to pay so that it knows whose balance to increase.)

Mining: A Definition

In Ethereum, miners refer to a vast global network of computers, operated mostly by enthusiasts in their homes and offices, running Ethereum nodes paid in ether tokens for the work of executing smart contracts and validating the canonical order of transactions around the world. Each node undertakes the process of mining. Still, the term also refers to the collective effort of the network: individual nodes mine, and the network itself can be said to be secured by mining.

Miners process transactions in groups known as blocks. We previously defined a block, in the abstract, as a collated set of transactions that take place over a given time. However, a block can also refer to the data object containing those transactions stored on Ethereum nodes. Each time a node starts, it must download the blocks it missed while offline. Each block contains some metadata from the previous block to prove it is authentic and build on the existing blockchain.

The “true” order of transactions is hard for the network to determine. New transactions may arrive at mining nodes in different parts of the world out of sequence. There exist many more incorrectly ordered blocks than correctly ordered ones. Some malicious node operators may modify their machines to submit fraudulent blocks in the hopes of sending free ether to their accounts.

Thus, mining can adequately be defined as dedicating computational effort to bolstering a given version of history as the correct one. The mining process computationally demands nodes because it involves executing a memory-intensive hashing algorithm known as a proof-of-work algorithm.

The proof-of-work algorithm (or PoW algorithm) for the Ethereum protocol is Ethash, a new function created by the core developers to address mining centralization evident in Bitcoin. You'll sometimes hear this algorithm referred to as Ethereum's consensus algorithm or consensus engine. The block that is chosen as canonical has the highest amount of proof of work behind it.

Hashpower refers to the amount of computation a miner can perform on the network. Hashpower reflects an individual computer's parts and specifications—in particular, the speed, power, and quantity of graphics processing cards; the computer system's overall power supply; and the availability of adequate voltage from the wall outlet and the breaker panel it's connected to.

The cryptographic proof which results from mining can be completed more quickly when more hash power is applied. Therefore, miners often form mining pools to increase their chances of winning rewards, which they then split among the group.

Versions of the Truth

To understand why there are so many versions of transaction history, let’s turn to Gavin Wood, who says it best in the Ethereum Yellow Paper:

Since the system is decentralized and all parties can create a new block on some older preexisting block, the resultant structure is necessarily a block's tree. There must be a consensus on which path through this tree structure, known as the blockchain, should be taken from root (the genesis block) to leaf (the block holding the most recent transactions).

Simply note that when nodes disagree about which root-to-leaf path is the true blockchain, then a state fork happens, and that is usually disastrous—the equivalent of the EVM splitting into two EVMs.

Difficulty, Self-Regulation, and the Race for Profit

Mining is designed to be a money-maker for the people who engage in it; they are paid for providing security to the network.

The first thing to know is that time is a factor. When a new cryptocurrency launches, miners rush to turn on their machines. With less competition for fees in the early days, they earn more. Even better, tokens belonging to useful crypto networks usually inflate in price over their lifetime, so earning them earlier gives miners more opportunity to profit from appreciation.

Difficulty

Ethereum and Bitcoin are self-regulating networks. As a network gets more popular, more mining hash power joins in search of profits, and blocks might be found too quickly. A dynamically self-adjusting value called difficulty would increase to stay within range of its ideal 15-second block time. If blocks are found too quickly or slowly, the system changes the difficulty to get within range of its ideal block time.

Generally speaking, as time progresses, network difficulty increases. However, the actual difficulty value is calculated with a formula that includes several variables. Network difficulty may decrease or go flat if miners drop off the network or reduce overall hash power.

After the Ethereum network experienced attacks in October and November 2016, the market price of ether dropped, and the hash rate was reduced as miners who couldn’t make a profit turned off their machines. It rose to its pre-attack highs several months later, commensurate with the recovery in the price of ether.

You can think of this difficulty variable as being part of the incentive structure to get miners on the network as soon as possible and to stay there. However, the difficulty has another use in the EVM, as one of several factors used to determine a block’s score, sometimes referred to as its heaviness. The heaviest or highest-scoring path through the transaction data structure can be said to be the longest, the one that most miners have historically converged upon as the true root-to-leaf path.

Factors Required for Block Validation

Each miner produces and validates a candidate block that comprises four pieces of information:

- This block's hash of the transaction ledger (as this machine heard about it)
- The root hash of the entire blockchain
- Block number since the chain started
- The difficulty of this block

If all these things check out, this block is a candidate for winning block. However, even with this information correct, the miner must still solve the proof-of-work algorithm. As you'll see, the algorithm is essentially a guessing game designed to take a certain amount of time in service of the ideal 15-second block time.

When the guess is correct, this correct value, or nonce, is the final condition to render a block true, canonical, and valid. The nonce is known as evidence of solving the proof-of-work algorithm.

How Proof of Work Aids in Block Time Management

Anyone who can optimize for the proof-of-work algorithm can find valid blocks faster, causing uncles to lag further and further behind. A small group of hardware companies has acquired a disproportionately huge amount of power over the network in the Bitcoin network by creating hardware specifically built to run the Bitcoin PoW algorithm. The centralization of mining efforts is highly profitable in Bitcoin because it allows these big miners to find blocks faster, reaping all the block rewards. Slower machines never get a chance to solve a block, and eventually, even their uncle blocks come in further and further behind the winning block. Uncle blocks are necessary for Ethereum to support the winning block. Because legitimate uncles are a requirement, it is difficult for the network to locate a true block as uncles lag.

Enter the Ethash algorithm: The Ethereum protocol's defense against mining hardware optimization. Ethash is a derivative of Dagger-Hashimoto, a memory-hard algorithm that can't be brute-forced with a custom application-specific integrated circuit (ASIC), like the kind that is popular with Bitcoin mining enterprises.

The memory-hardness of this approach is due to the use of a directed acyclic graph (DAG) file, which is generally a 1 GB dataset that is recreated every 125 hours, or 30,000 blocks. This period of 30,000 blocks is also known as an epoch.

A directed acyclic graph is a technical term for a tree in which each node is allowed to have multiple parents, with ten levels including the root

and a total of up to 225 values.

What’s going on with the DAG and Nonce?

In effect, each node is playing a guessing game with itself, trying to guess a nonce that will validate the current block; if it guesses the correct nonce, it wins the block reward. If not, it continues guessing until it gets word that another node on the network has found a winner. Then, it discards the block it was mining, downloads the new block, and begins mining a new block on top of that one. But the node gets both parameters of the guessing game and a new pair of dice (so to speak) with each potential block as it rolls in. The rules of the guessing game are designed to prevent clever individual nodes from outsmarting the system in the pursuit of more mining rewards.

Therefore, you can think of the DAG file to standardize the solution time of the proof-of-work algorithm. It levels the playing field for miners, but more importantly, helps cluster block times around the 15-second mark by ensuring that—even with massive computing power—you can’t guess the correct nonce a whole lot faster than your competitors.

All the data a node needs to participate in the guessing came is drawn from the blockchain itself. An encryption seed can help generate a pseudorandom number in cryptography, thus increasing the randomness of whatever encrypted output the Ethash algorithm produces. In Ethereum and Bitcoin, each node gets the seed from looking at the last known winning block hash. In this way, the node must be mining on the correct, canonical chain to play the game correctly. Performing proof of work on an erroneous block (say, an uncle) cannot yield a winning block. This is helpful if you’re trying to reduce unfair advantage in a proof-of-work scheme, which a large pool of miners could use to highjack the network onto a version of the truth in which everyone’s ether is transferred to the hijacker’s accounts. Here is the

process by which a node sets itself up to perform the PoW guessing game:

1. From an encryption seed derived from the block header, the mining node creates a 16 MB pseudorandom cache.

2. In turn, the cache is used to generate a more significant 1 GB dataset that should be consistent from node to node; this is the DAG. This dataset grows over time, linearly, and is stored by all full nodes.

3. Guessing the nonce requires the machine to grab random slices of the DAG dataset and hash them together. This works similarly to using a salt with the hash function.

In cryptography, a random data chunk you toss into a one-way hash function is called a salt. Salts are like nonces: they make things more spontaneous and thus more secure.

All This for Faster Blocks?

Believe it or not, all these modifications to the original Bitcoin paradigm were made in the service of faster block times. Block times as low as 3–5 seconds may be mathematically feasible.

In both Bitcoin and Ethereum, we've said that block time is an idealized period for collecting transactions. Why is this? The system works to keep blocks as near as possible to the ideal, much like the human body tries to preserve homeostasis.

The Bitcoin protocol targets 10-minute block times, and Ethereum targets 15 seconds. Once a valid block is found, it takes a short while for other nodes to find out about it. Until they discard their orphan block and begin mining on the new one, they compete against the new block instead of building upon it. Thus, the effort expended on the orphan is wasted. Think of it this way: if latency causes miners to hear about new blocks an average of one minute late, and new blocks come every 10 minutes, the overall network wastes roughly 10 percent of its power. This waste is reduced by increasing the duration between blocks. In the opinion of some blockchain theorists, Satoshi Nakamoto chose this ratio because it seemed an acceptable level of waste. Ethereum faster blocks time is desirable because it makes transactions confirm more quickly. Still, the Ethereum protocol has had to make provisions in its design for the proportional decrease in security brought on by faster block times, as you'll see later in this chapter. Block time can be compared to settlement time in securities trading, which in the United States stands at three days after the trade date, also known as T+3. A proposal is under consideration by the SEC to quicken settlement time to T+2.

In Bitcoin, which has no smart-contract execution, blocks take a theoretical 10 minutes on average, but in reality, transactions process this quickly only about 63 percent of the time. About 13 percent of the time, it takes longer than 20 minutes for a transaction to receive confirmation. During this time, it’s possible to reverse a transaction up to 20 percent of the time.

While merely irksome for Bitcoin enthusiasts and businesses, these conditions are unacceptable for a smart-contracts platform designed to power distributed software applications, so Ethereum takes a slightly different approach to mine to achieve faster block times.

Making Fast Blocks Work

Because nodes are located worldwide, it’s hard for them to stay perfectly in sync. That’s because information takes time to travel across the Internet from node to node, also known as latency. Although it may not seem like much time to humans, it’s enough to create collisions in the transaction record where the books don’t balance.

On average, it takes about 12 seconds for a transaction to propagate around the Ethereum or Bitcoin networks; in actuality, much of this time is consumed by downloading transactions to the node.6 In the intervening time before it hears about a new block being found, a miner may continue to work on an old block briefly before discarding it for the new winner. As described in the section above, uncles that receive mining effort after a valid block has already been found elsewhere in the network are also known as stale or extinct blocks.

Faster block times create a higher likelihood of stale blocks, and stale blocks decrease the network’s absolute strength against attacks.7 Worse yet, higher rates of stale blocks make it easier for mining pools to win, increasing efficiency advantages over solo miners, consistently beating them out of mining rewards. At best, this is unfair, and at worst, it makes the network less expensive to attack.

References

Anonymous. (2017). *The Secret to Making Money with Bitcoin and Ethereum.*

Bonello, P. (2021). *Valuing Ethereum.* Grayscale.

Breitman, K., & Brown, R. (n.d.). *Ethereum: Platform Review*.

Buterin, V. (n.d.). *Ethereum White Paper*.

Coindesk. (2016). *Understanding Ethereum.* Coindesk.

Ethtrade.com. (n.d.). *Understanding Ethereum.*

Etoro. (n.d.). *Ethereum: A Beginners Guide.*

Solomon, M. G. (2019). *Ethereum for Dummies.* USA: John Wiley and Sons.

TutorialsPoint.com. (2019). *Ethereum.* TutorialsPoint.Ltd.

Atzei, N., Bartoletti, M., & Cimoli, T. (2016). *A survey of attacks on Ethereum smart contracts.*

Buterik, V. (2017). The Meaning of Decentralization. *Medium*.

Castillo, M. (2016). *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft.* Coindesk.

Castor, A. (2018). *The Ethereum ICO: Where did all the tokens go?"*. The Block.

Curran, B. (2019). *The Complete Beginner's Guide to Ethereum.* Blockonomi.com / Kooc Media Ltd.

Gracyscale.co. (2021). *Valuing Ethereum*

Lee, C. (2017). *CRYPTOCURRENCY:BITCOIN, ETHEREUM, BLOCKCHAIN HOW TO GUIDE:INVESTING, TRADING, MINING.*

Maurya, S. (2019). *"Embracing Web 3.0: The New Internet Era Will Begin Soon."*. Hacker Noon.

Taleb, N. (n.d.). *Things, That Gain from Disorder.*

The Financial Freedom Foundation Org. (2018). *Cryptocurrency Evolution.* Financial Freedom Foundation Org.